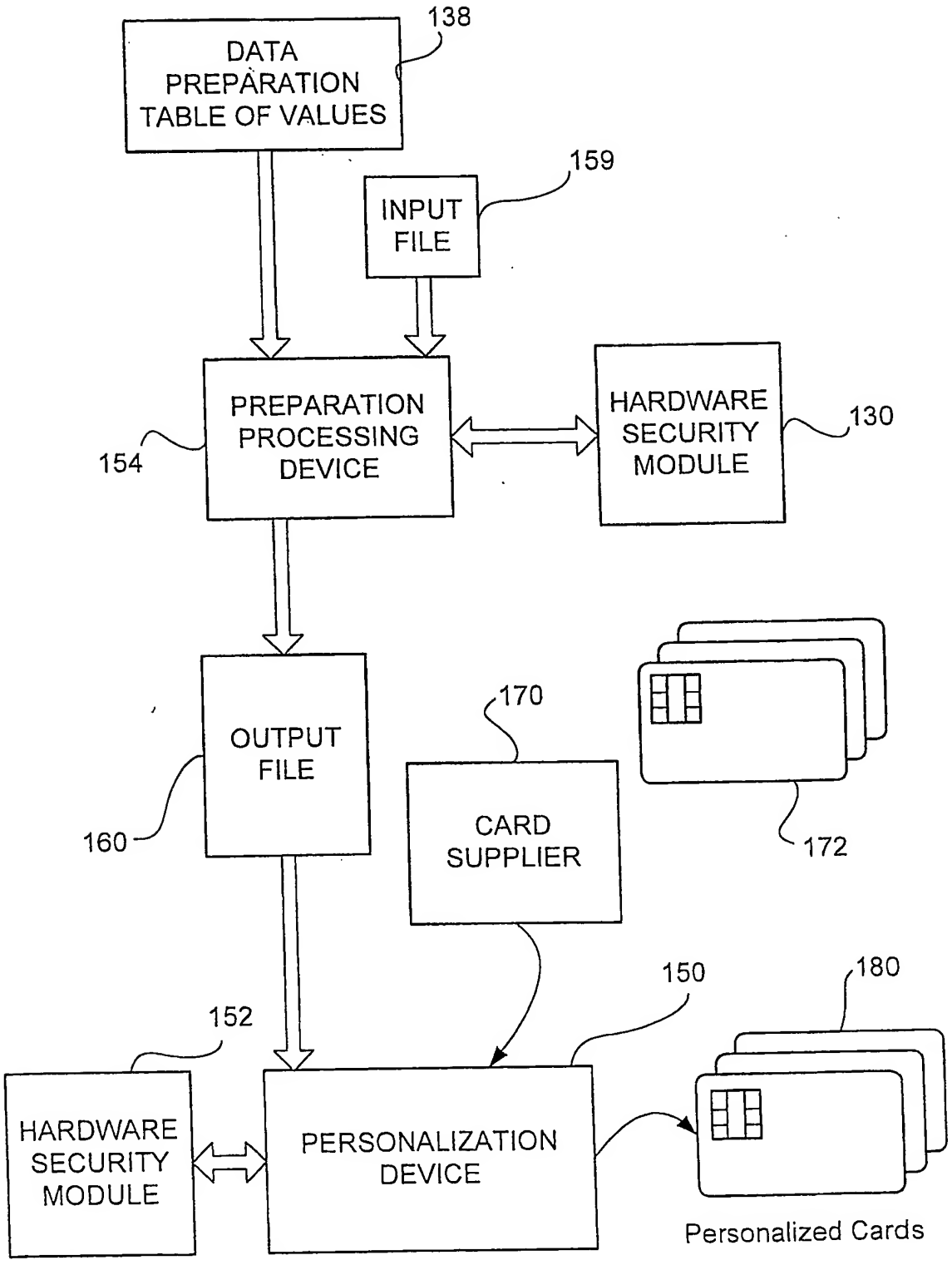


FIG. 1 (PRIOR ART)

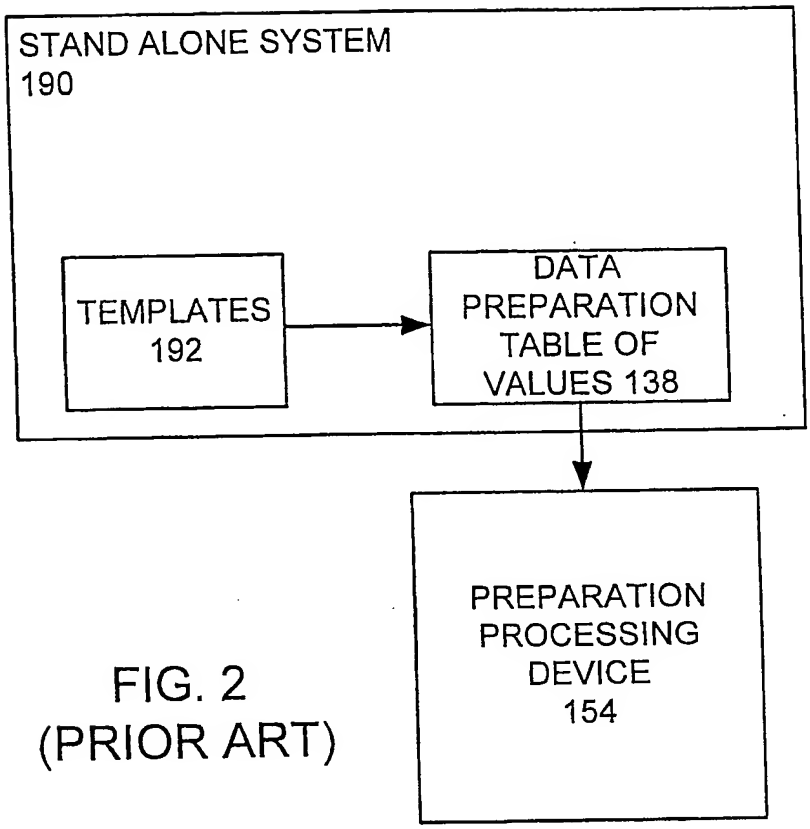


FIG. 2
(PRIOR ART)

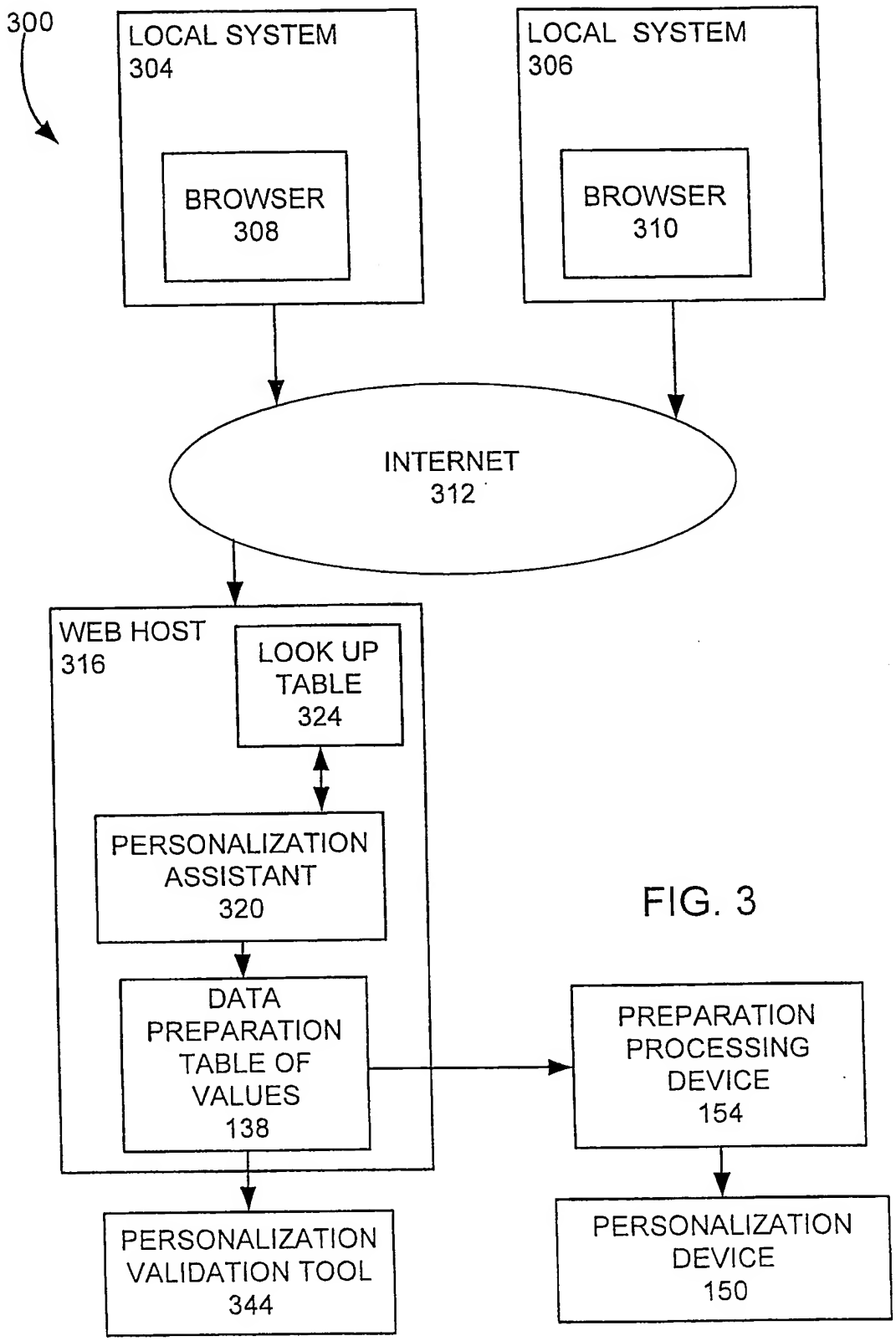

300
LOCAL SYSTEM
304
BROWSER
308
LOCAL SYSTEM
306
BROWSER
310
INTERNET
312
WEB HOST
316
LOOK UP
TABLE
324
PERSONALIZATION
ASSISTANT
320
DATA
PREPARATION
TABLE OF
VALUES
138
PERSONALIZATION
VALIDATION TOOL
344
PREPARATION
PROCESSING
DEVICE
154
PERSONALIZATION
DEVICE
150

FIG. 3

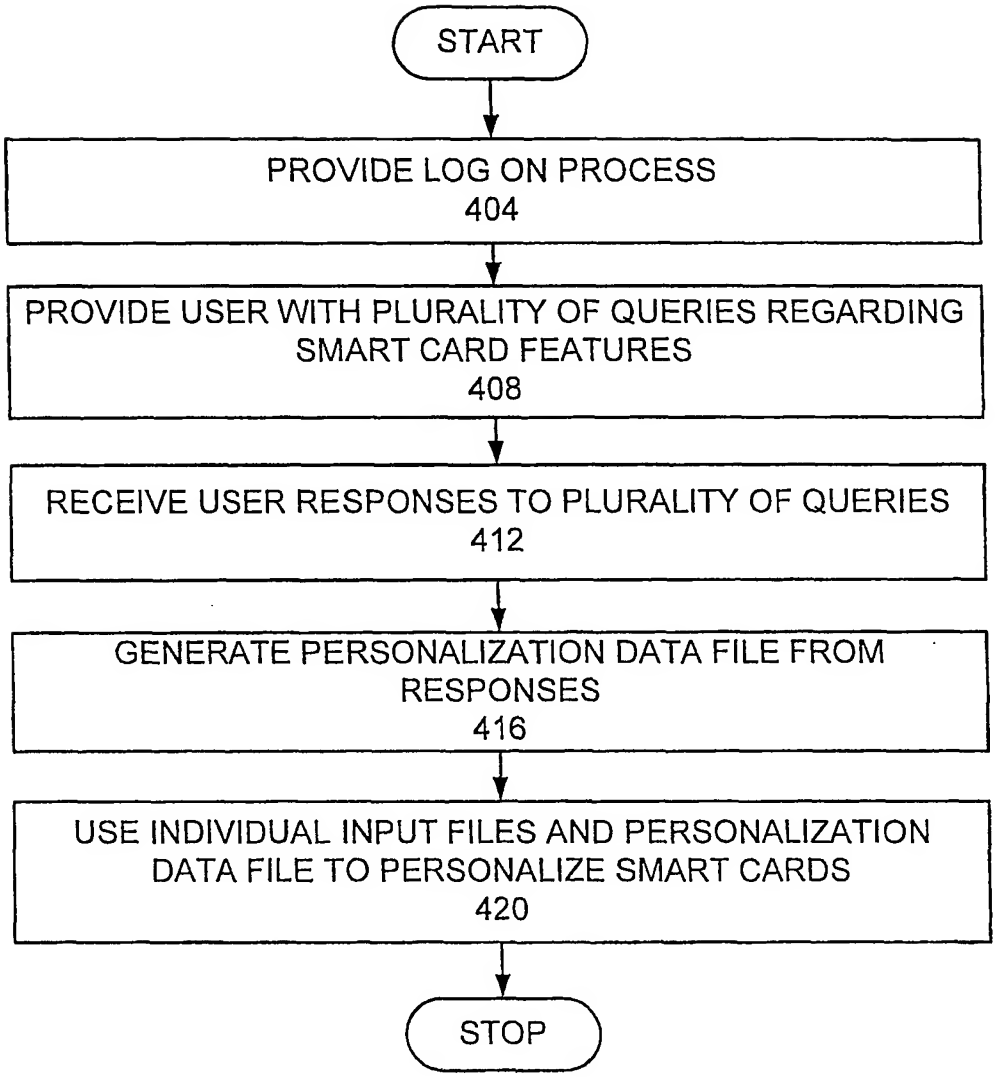

START
PROVIDE LOG ON PROCESS
404
PROVIDE USER WITH PLURALITY OF QUERIES REGARDING SMART CARD FEATURES
408
RECEIVE USER RESPONSES TO PLURALITY OF QUERIES
412
GENERATE PERSONALIZATION DATA FILE FROM RESPONSES
416
USE INDIVIDUAL INPUT FILES AND PERSONALIZATION DATA FILE TO PERSONALIZE SMART CARDS
420
STOP

FIG. 4

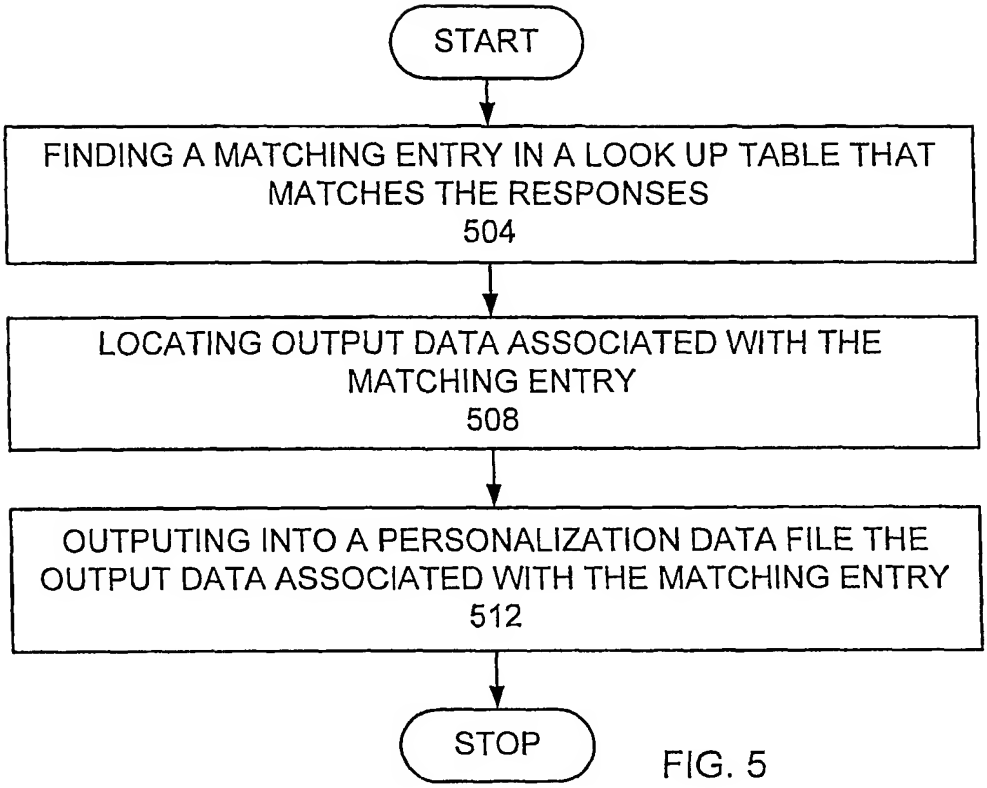

START
FINDING A MATCHING ENTRY IN A LOOK UP TABLE THAT MATCHES THE RESPONSES
504
LOCATING OUTPUT DATA ASSOCIATED WITH THE MATCHING ENTRY
508
OUTPUTING INTO A PERSONALIZATION DATA FILE THE OUTPUT DATA ASSOCIATED WITH THE MATCHING ENTRY
512
STOP

FIG. 5

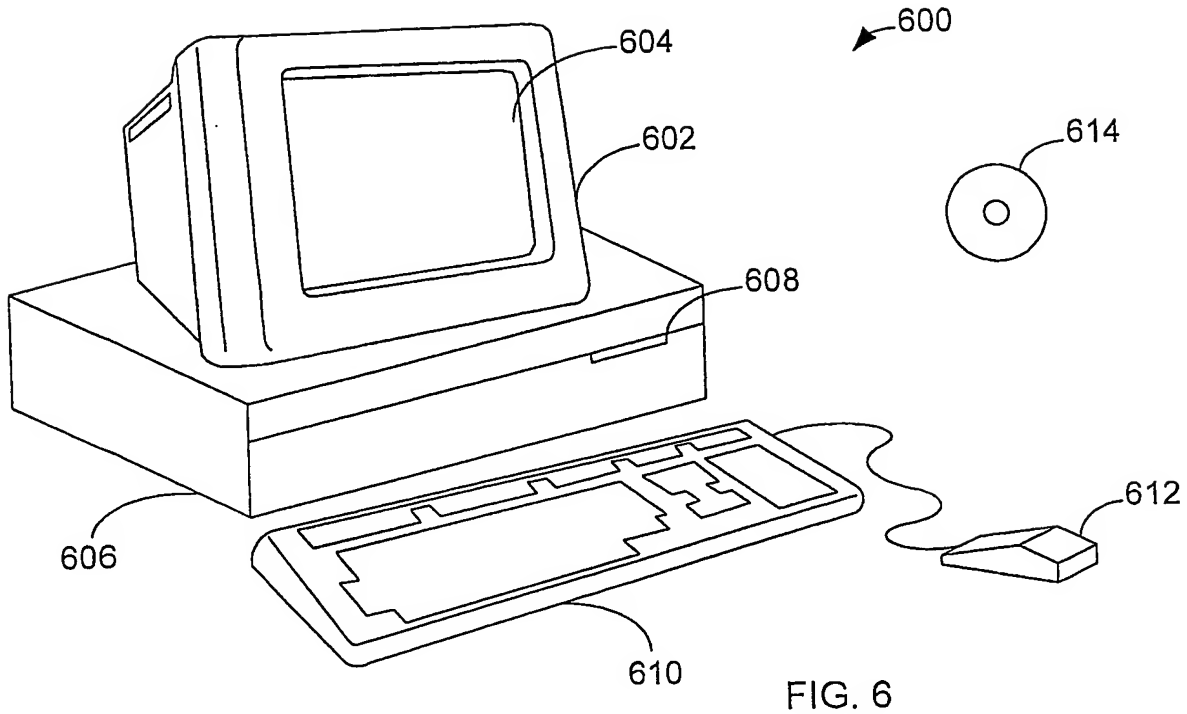

600
604
602
614
608
612
606
610

FIG. 6

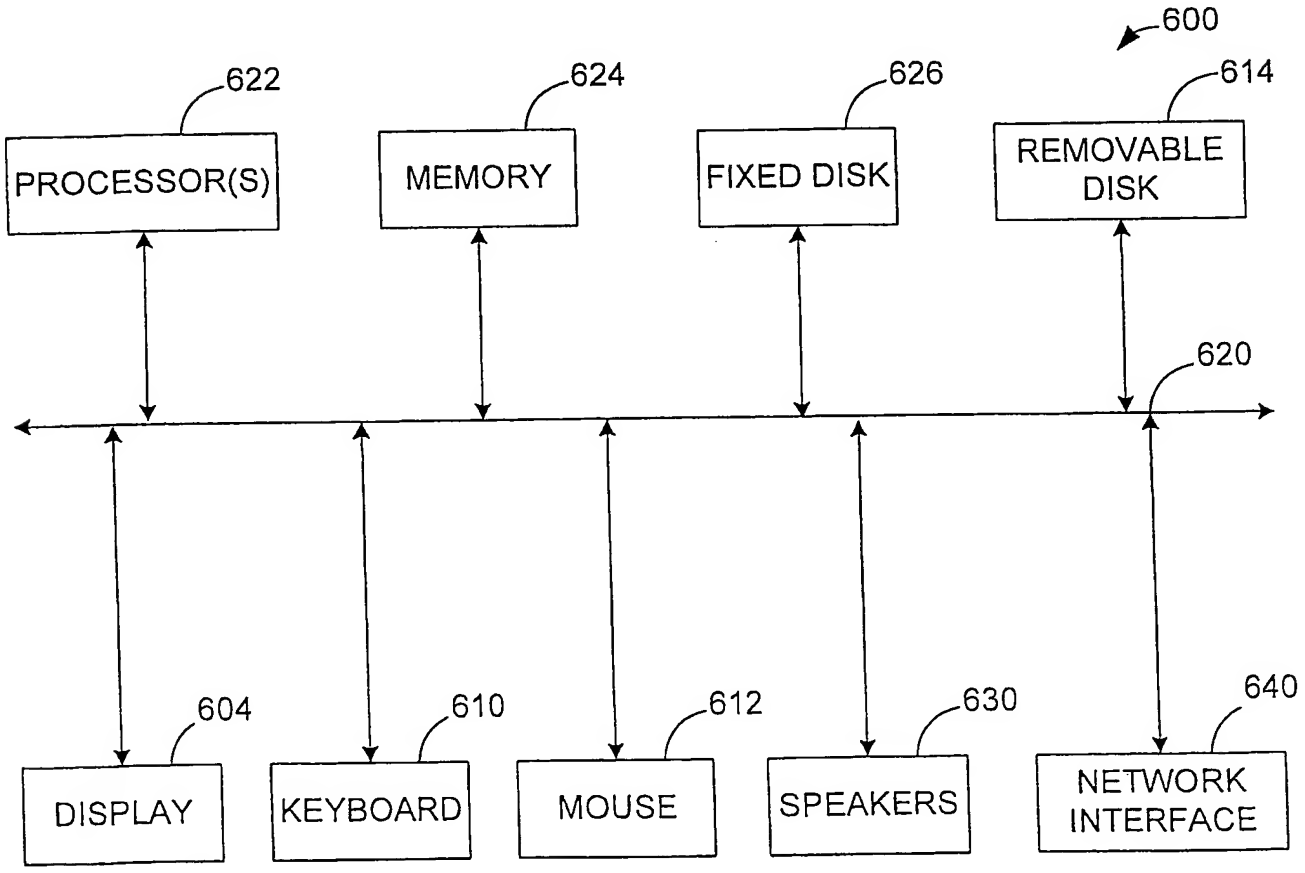

600
622
624
626
614
PROCESSOR(S)
MEMORY
FIXED DISK
REMOVABLE DISK
620
604
610
612
630
640
DISPLAY
KEYBOARD
MOUSE
SPEAKERS
NETWORK INTERFACE

FIG. 7

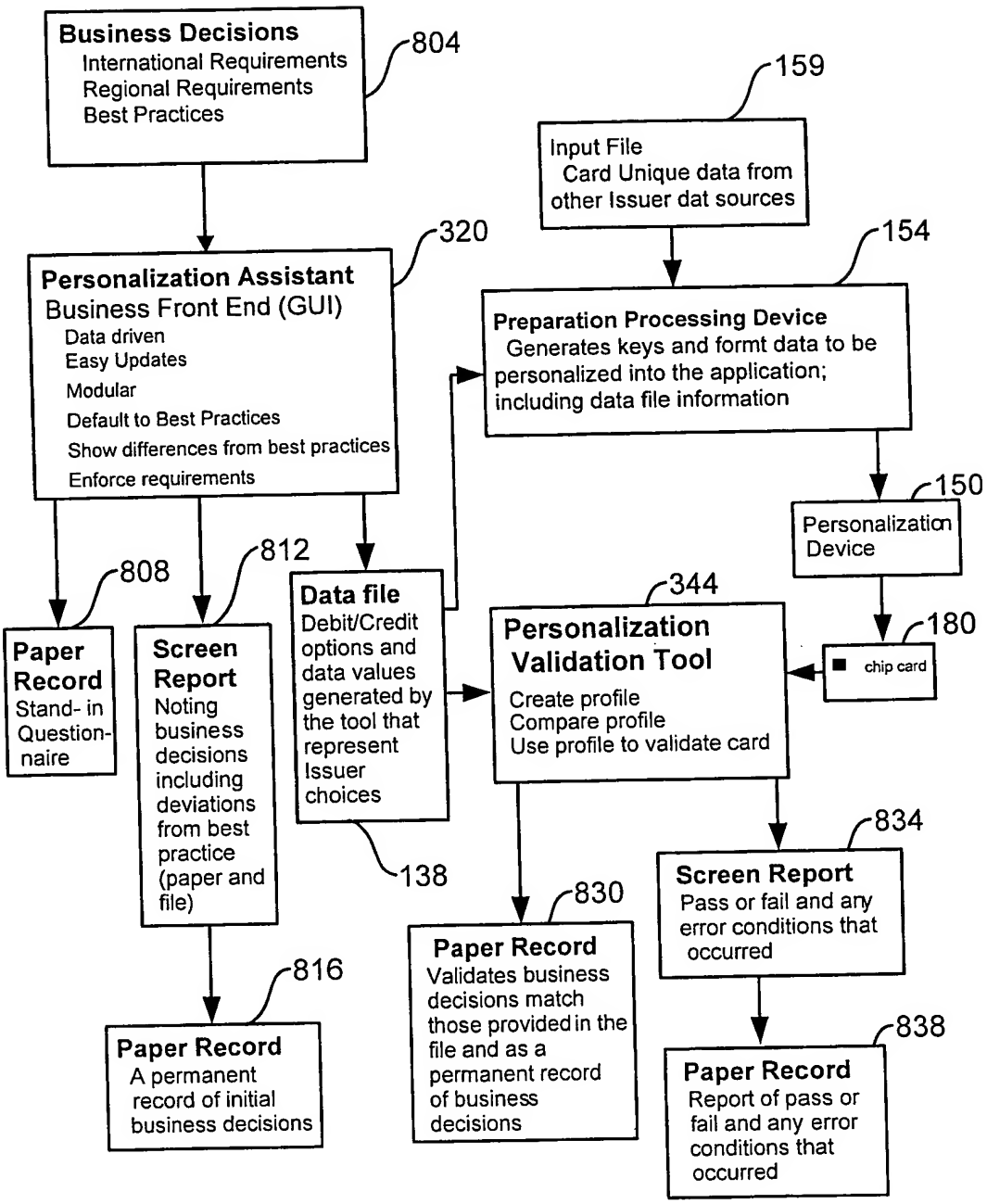

Business Decisions
International Requirements
Regional Requirements
Best Practices
804
159
Input File
Card Unique data from other Issuer dat sources
320
Personalization Assistant
Business Front End (GUI)
Data driven
Easy Updates
Modular
Default to Best Practices
Show differences from best practices
Enforce requirements
154
Preparation Processing Device
Generates keys and formt data to be personalized into the application; including data file information
150
Personalization Device
808
812
Data file
Debit/Credit options and data values generated by the tool that represent Issuer choices
344
Personalization Validation Tool
Create profile
Compare profile
Use profile to validate card
180
chip card
Paper Record
Stand- in Question-naire
Screen Report
Noting business decisions including deviations from best practice (paper and file)
138
834
Screen Report
Pass or fail and any error conditions that occurred
830
Paper Record
Validates business decisions match those provided in the file and as a permanent record of business decisions
816
Paper Record
A permanent record of initial business decisions
838
Paper Record
Report of pass or fail and any error conditions that occurred

FIG. 8

VSDC Personalization Assistant Database (Phase I):

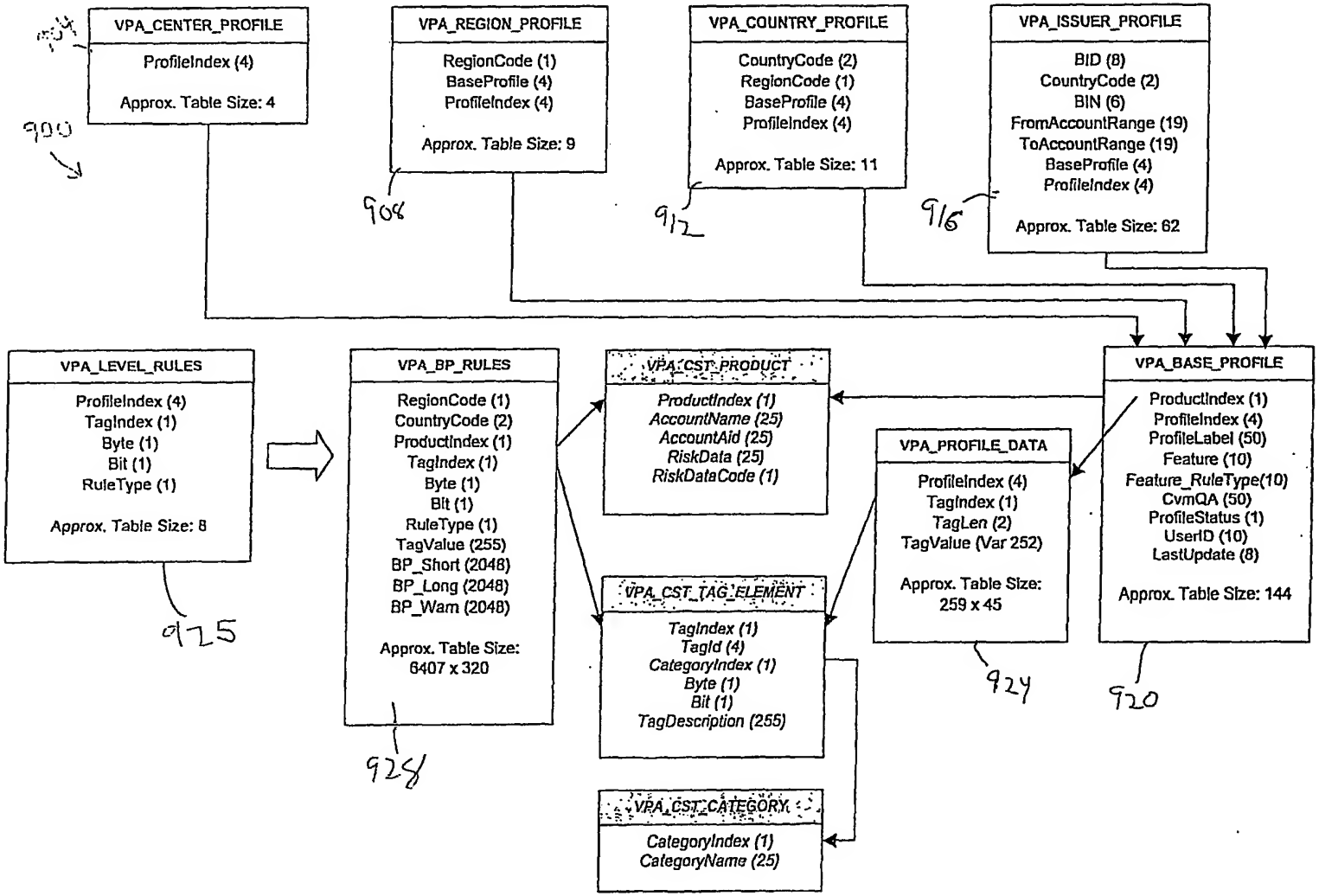
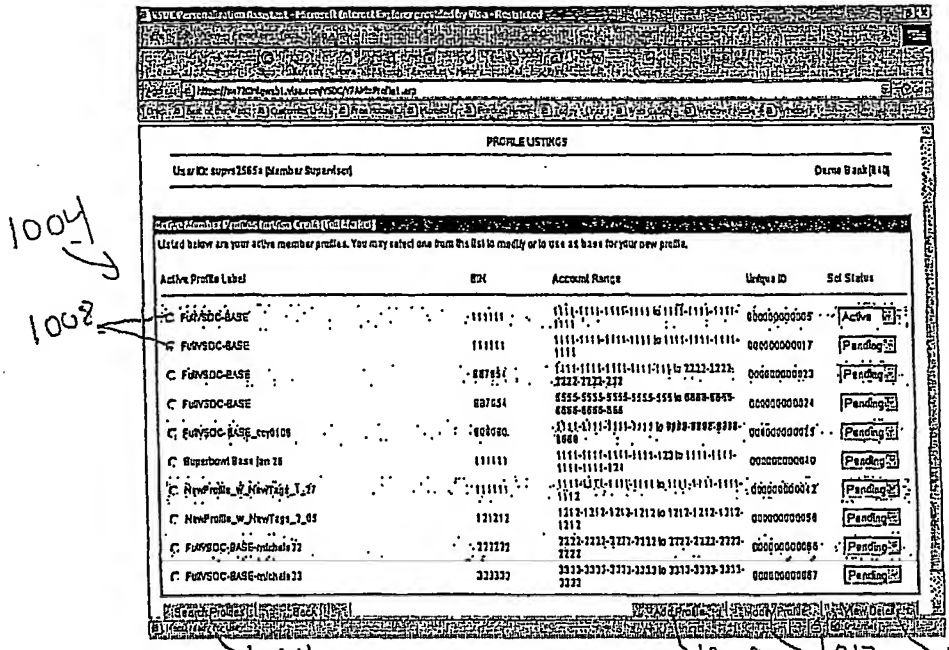


FIG.9



At any point on this screen, the user may click on Back to return to the previous screen.

FIG. 10

6.5.1.1 View Details

In the Profiles Listing screen, the user may select one of the profiles listed and click on the View Details button to obtain details on how the selected Member profile was configured. The user will be taken to the Reports Selection screen where a choice of reports may be viewed or printed. The user may also navigate through all VPA screens, but will only have read-access to the features selected. None of the selected features can be changed in this mode.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

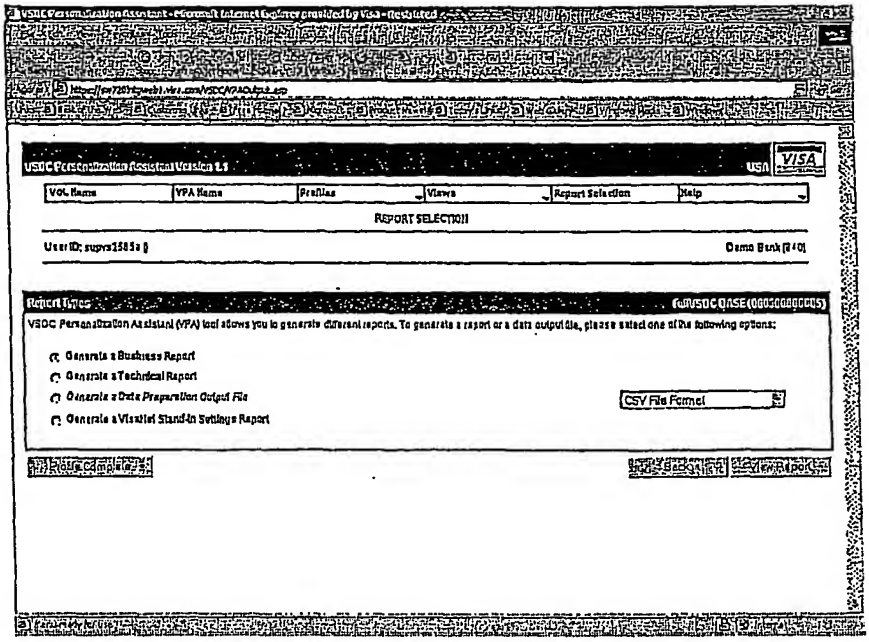


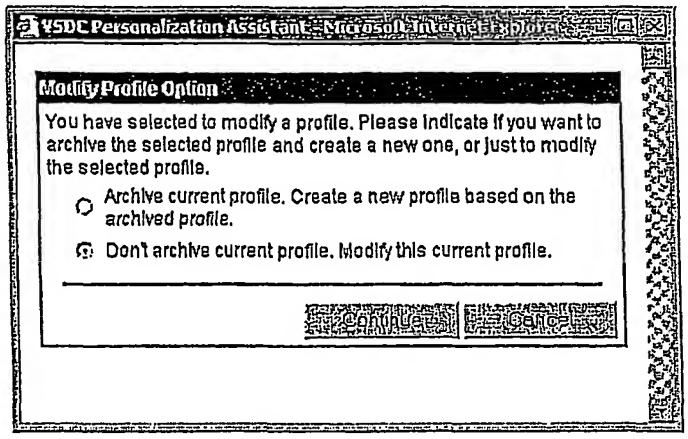
FIG. 11

More details on the Reports Selection screen is provided in Section 6.7.

6.5.1.2 Modify Profile

From the Profiles Listing screen, the user may choose to modify one of the profiles listed. On selecting a profile and clicking on the Modify Profile button, the user will be presented with the following screen:

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.



1204

Here the user may choose either to archive the selected profile and create a new one using the archived profile as its base, or to modify the selected profile without archiving it.

FIG. 12

Note:

Profiles modified by the user will remain in a PENDING state until the configuration process has been completed. On completion of the process, the user can move the profile to an ACTIVE state.

On making the appropriate selection, the user should click on the Continue button.

6.5.1.3 Add Profile

If the user chooses to add a new profile, a box will appear requesting the following information be entered:

- Profile Label
- Member BIN
- Account Range ('to' and 'from')

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

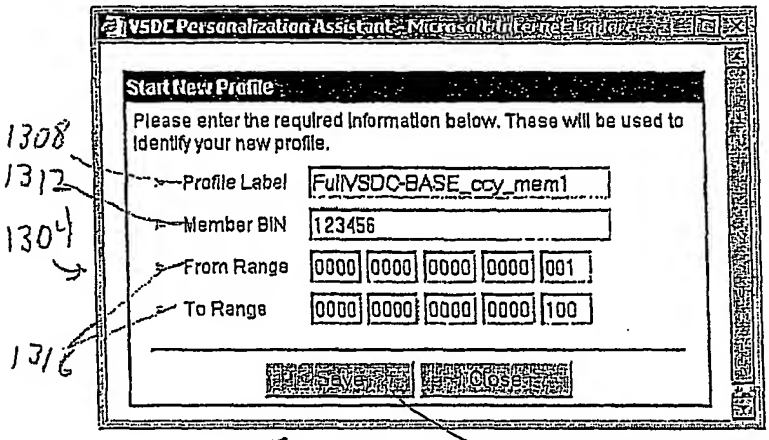


FIG. 13

Note:

New profiles added by the user will remain in PENDING state until the configuration process has been completed. On completion of the process, the user can move the profile to an ACTIVE state.

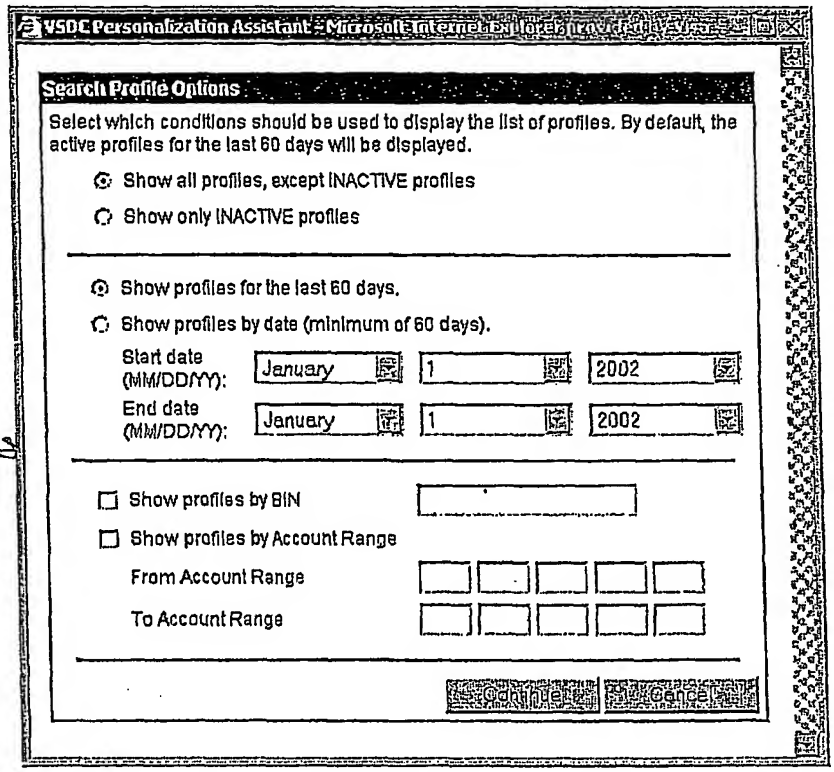
After all requested information has been entered, the user should click on the Save button to proceed to the next screen.

The next screen provides the user with a summary of selected VSDC features based on the default profile. For information on this screen please refer to Section 6.6.

6.5.1.4 Search Profile

The 'Search Profile' feature allows the user to search from a list of 'Active' or 'Inactive' profiles over a period defined by the user. The user may search by Bank Identification Number (BIN) or Account Range.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.



1404

FIG. 14

To perform a search, the user should enter the required information and click on the Continue button to proceed.

6.5.2 Using a Visa-recommended Profile

From the Business Profile Selection screen, the user may choose a Visa-provided default profile as the base for creating their Member Profile. This option is the only one available to first time users of VPA, and in cases where no pre-defined Member Profiles exist. If this option is chosen, the user only has the options to:

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

1. View Details: allows the user to view configuration details of the Visa default-profile. All functions are as described in Section 6.5.1.1 above.
2. Add Profile: allows the user to create a new profile based on a Visa default profile. All functions are as described in Section 6.5.1.3 above.

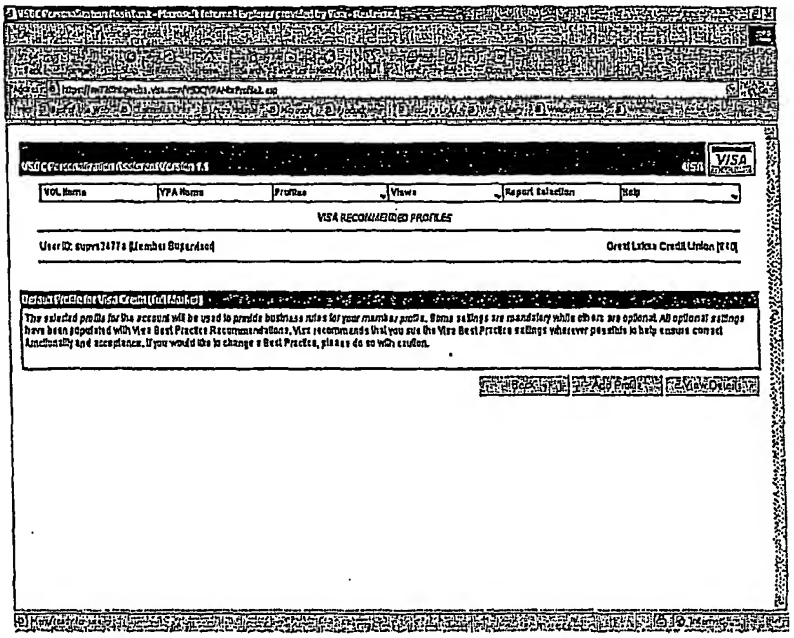


FIG. 15

6.6 VSDC Feature Selection

On completion of the profile selection process that defines the default profile to be used for building the new profile, VPA will present the user with the VSDC Feature Selection screen. This screen outlines the mandatory features that must be supported by the Issuer along with optional features that users can select or deselect.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

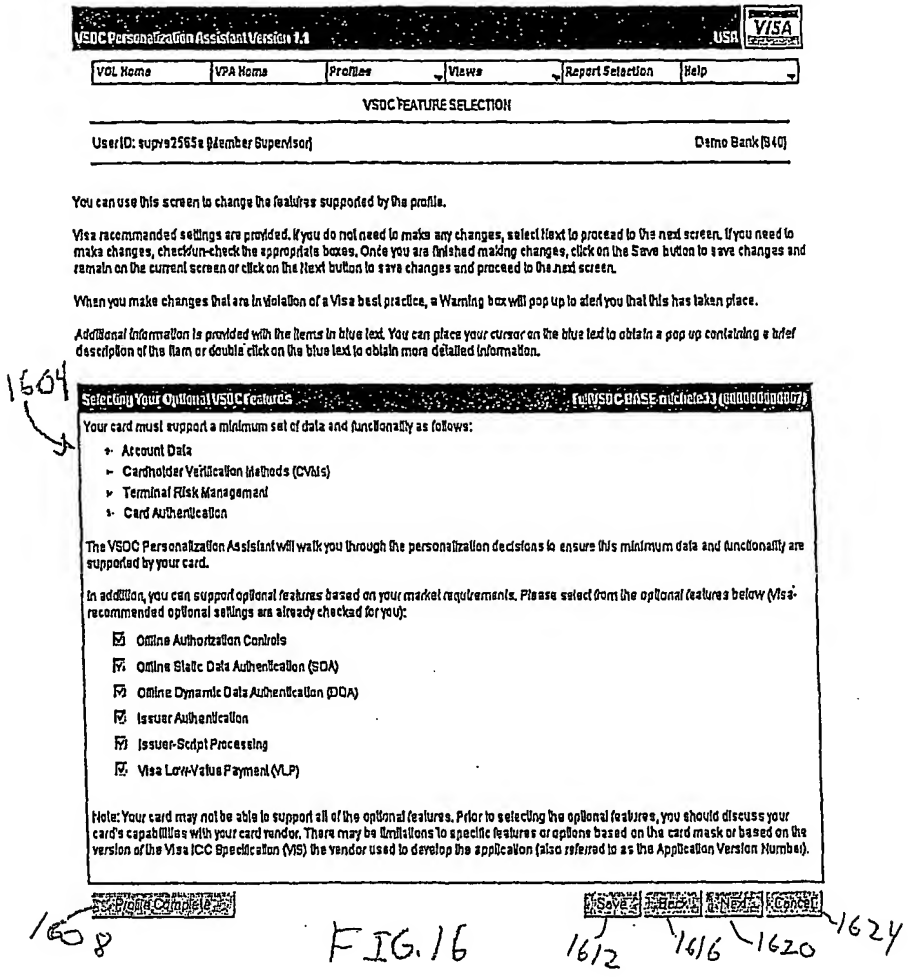


FIG. 16

Note:

If during the process of selecting or deselecting a feature or function the user changes an option that results in a violation of a current Visa best practice, VPA will provide a warning box to the user alerting them to the violation. The user then has the opportunity to alter this selection, or to continue by ignoring the violation.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

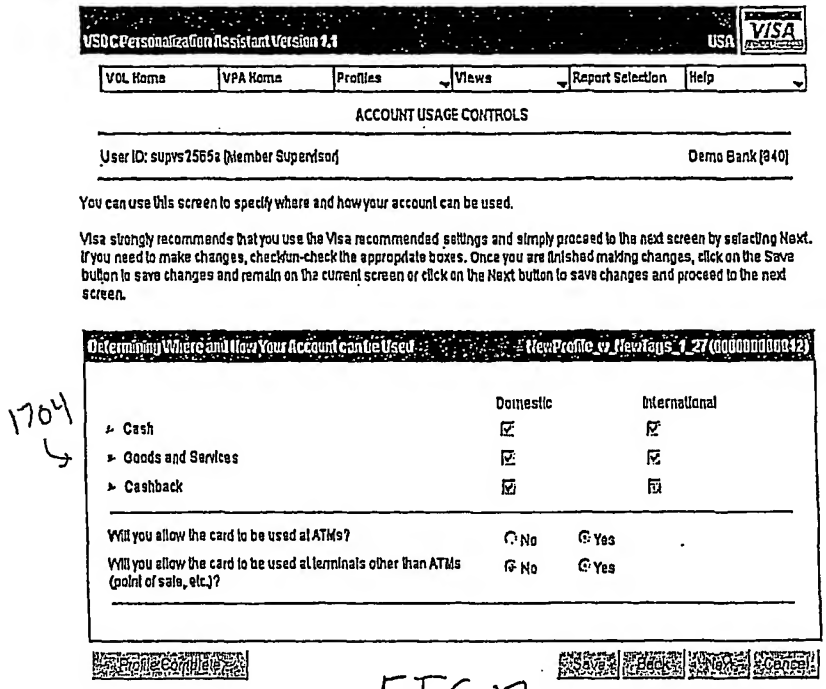
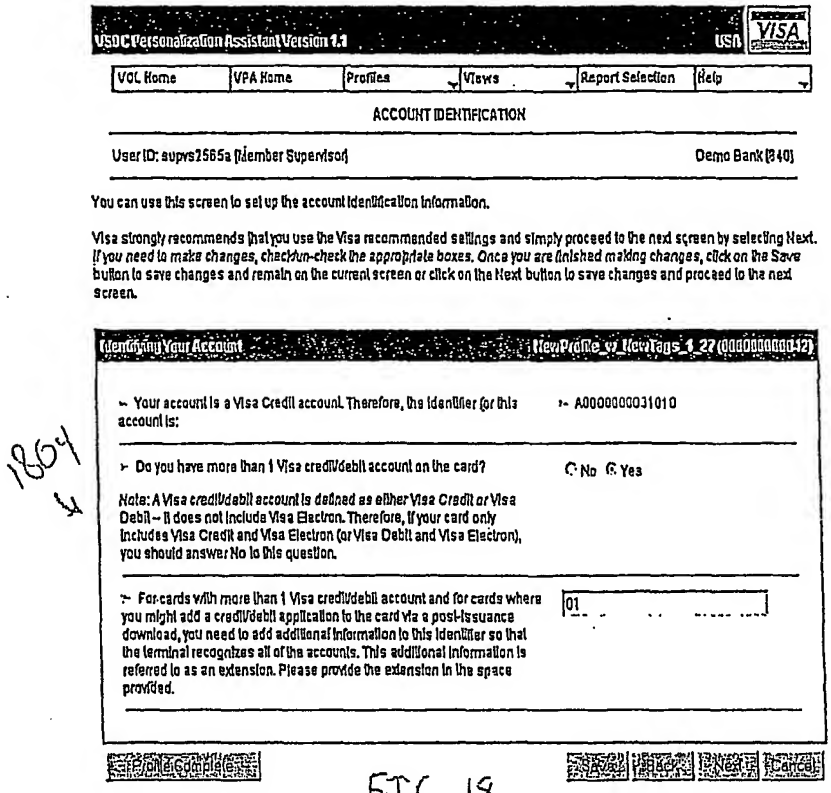


FIG. 17

6.6.2 Application Identification

For Issuer who choose to have more than one credit or debit application (using the same Application Identifier for each) on their card, this screen allows the user to uniquely identify each of these application using additional information referred to as the Application Identifier Extension.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.



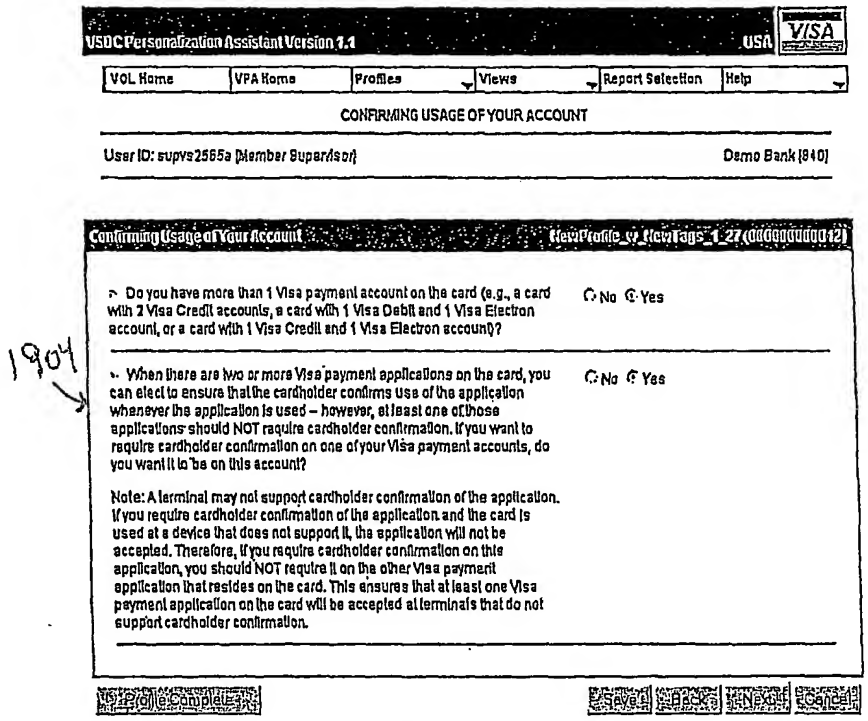
1864

FIG. 18

6.6.3 Application Confirmation

This screen allows the user to indicate whether there are multiple payment applications on the card. If multiple applications are present, the user has the option on this screen to set the currently configure application to require that the cardholder confirm the application's use before a transaction is performed.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.



1904

FIG. 19

Note:

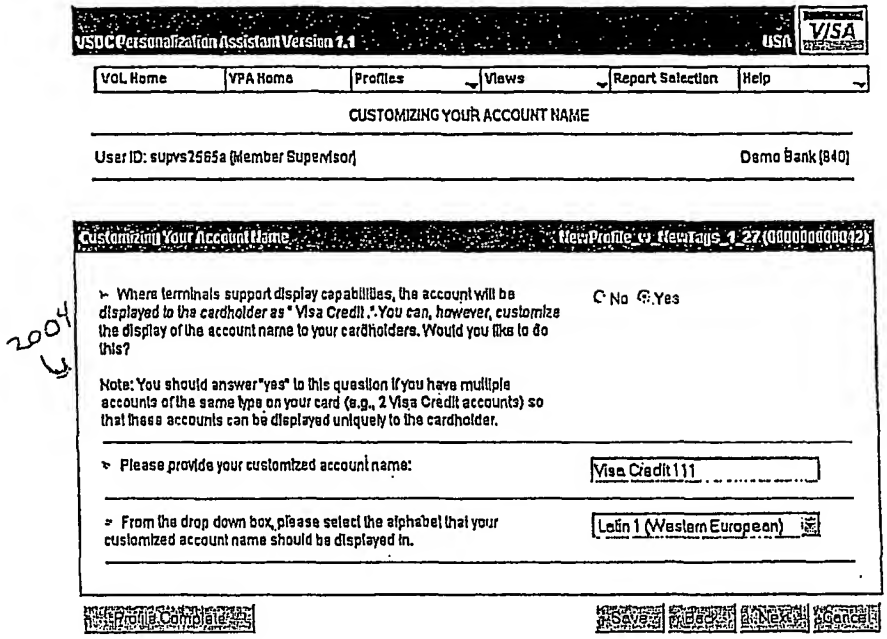
An EMV terminal may not support cardholder confirmation. If cardholder confirmation is required on an application and the card is used at a device that does not support it, the application will not be selected. Therefore, if cardholder confirmation is required on this application, the user should NOT require it on other Visa payment applications that reside on the card. This ensures that at least on Visa payment application on the card will be accepted at terminals that do not support cardholder confirmation.

6.6.4 Customizing Account Name

This screen allows the user to customize the account name of the application to be displayed in a specified language of choice, so that, in the event the terminal

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

supports the language of choice, the account name would be displayed to the cardholder in that language.



2004

FIG. 20

6.6.5 Customizing Account Language

This screen allows the Issuer to define up to four languages of choice, so that in the event the terminal in use supports any of these languages, the display messages provided by the terminal will be displayed in the chosen language.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

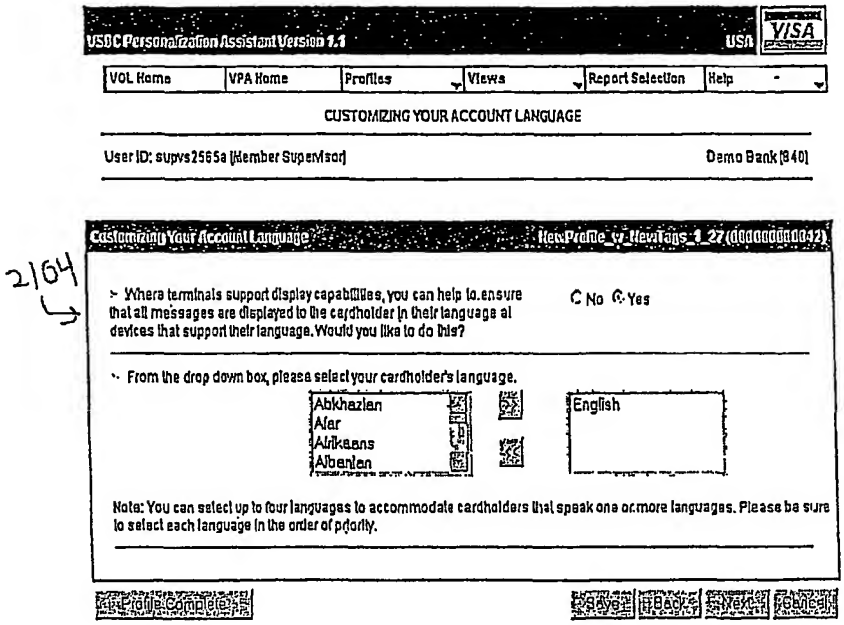


FIG. 21

6.6.6 Prioritizing the Account

This screen allows the user to set the required priority order by which the terminal should select the application, assuming that multiple payment applications are being supported on the card.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

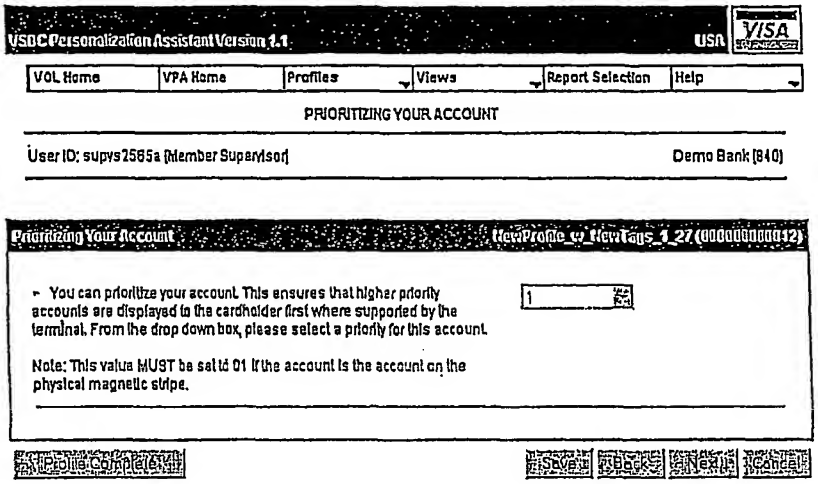


FIG. 22

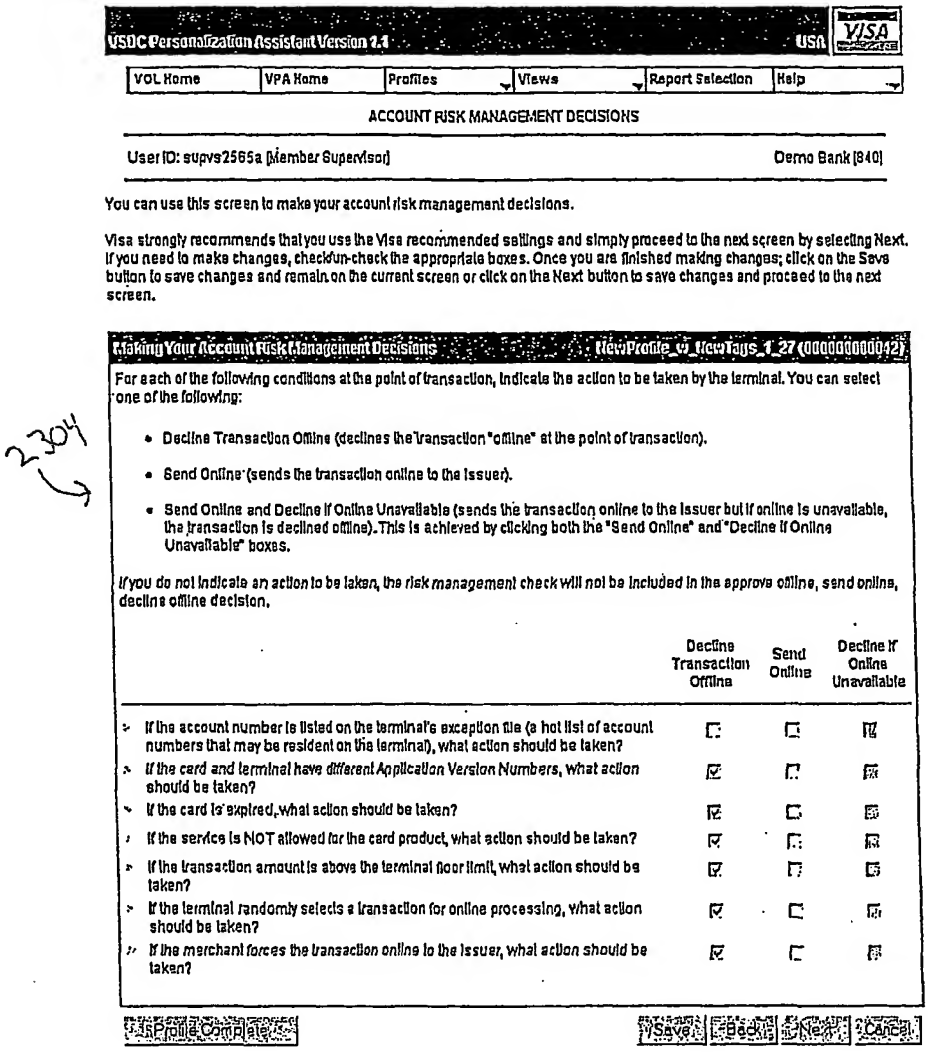
Note:

This value MUST be set to '01' if the account is the same one as reflected on the magnetic stripe.

6.6.7 Account Risk Management Decisions

This screen allows the user to set either decline offline, send online, or decline if online unavailable for various risk management results that may be detected by the terminal during transaction processing.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.



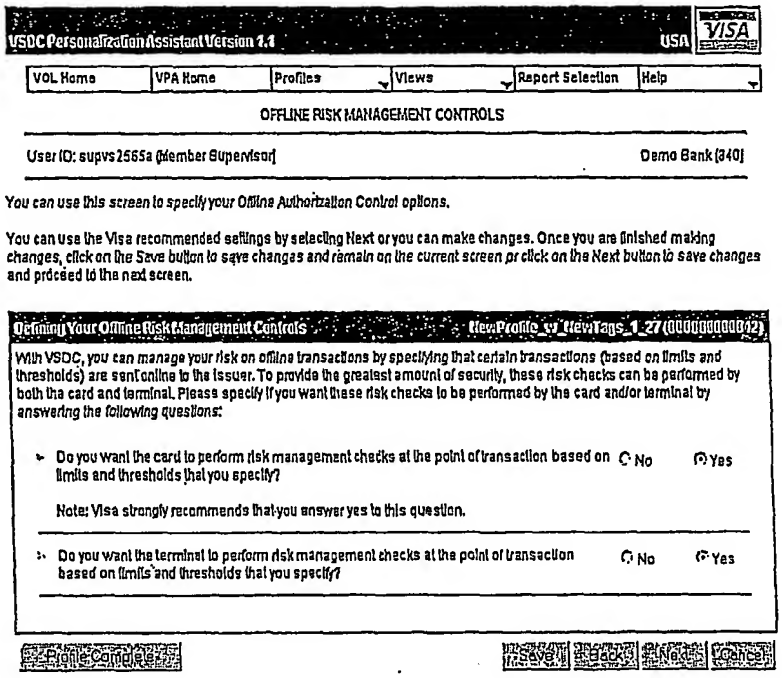
2304

FIG. 23

6.6.8 Offline Risk Management Controls

This screen allows the user to specify whether the card, terminal or both should perform velocity checking.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.



Note: FIG, 24

Visa strongly recommends that the user select the card to perform velocity checking.

6.6.8.1 Offline Limits and Thresholds – Card and Terminal Velocity Checking

This screen allows the user to select the appropriate Counter Limits, Amount Limits, Secondary Currency definitions, etc. that are required for Card and Terminal Velocity Checking.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

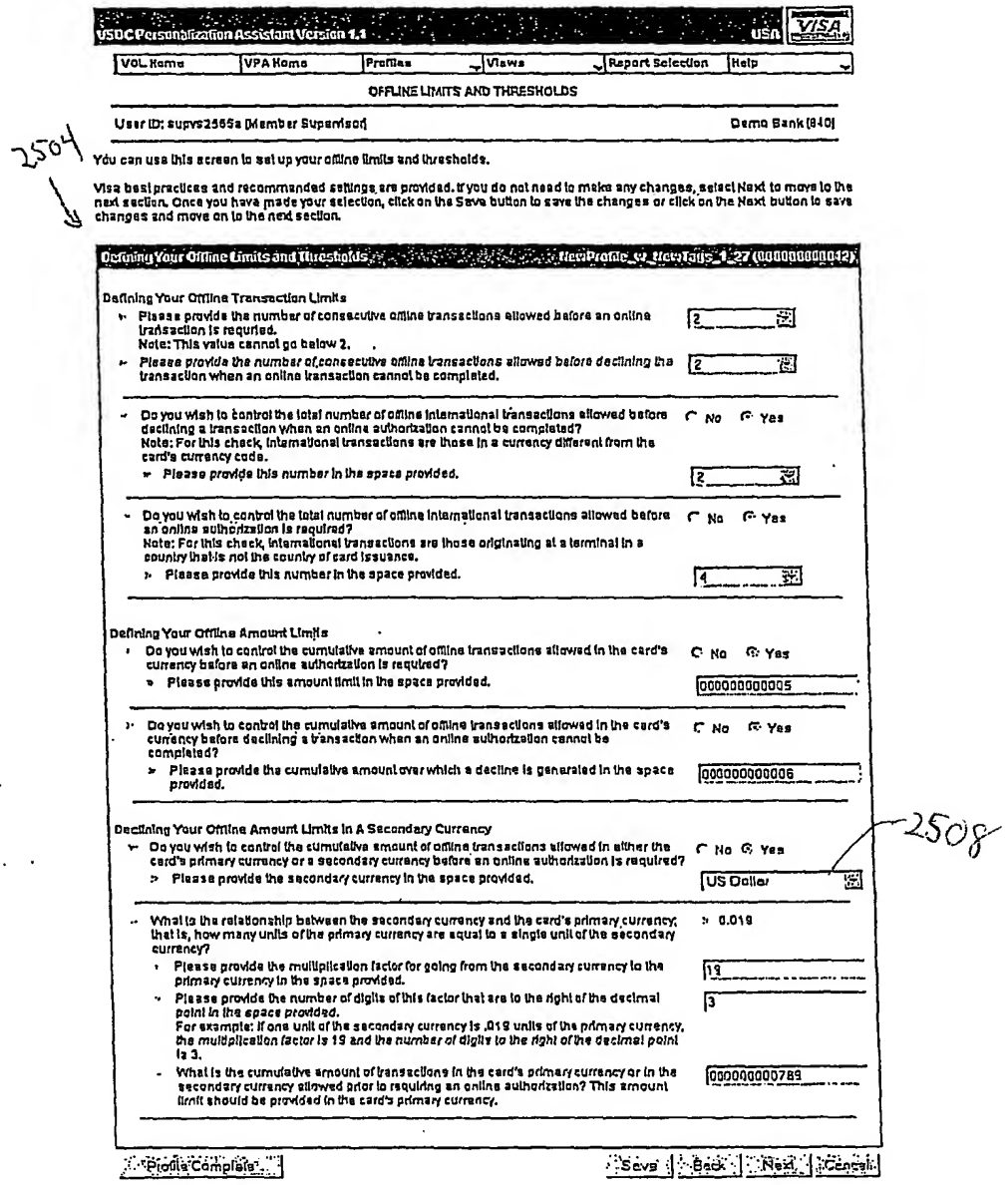


FIG. 25

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.6.9 Account Effective Date Checking

This screen allows the user to determine if an Application Effective Date is required on the account and the action to be taken if the cardholder attempts to use the card before the account becomes effective.

2604

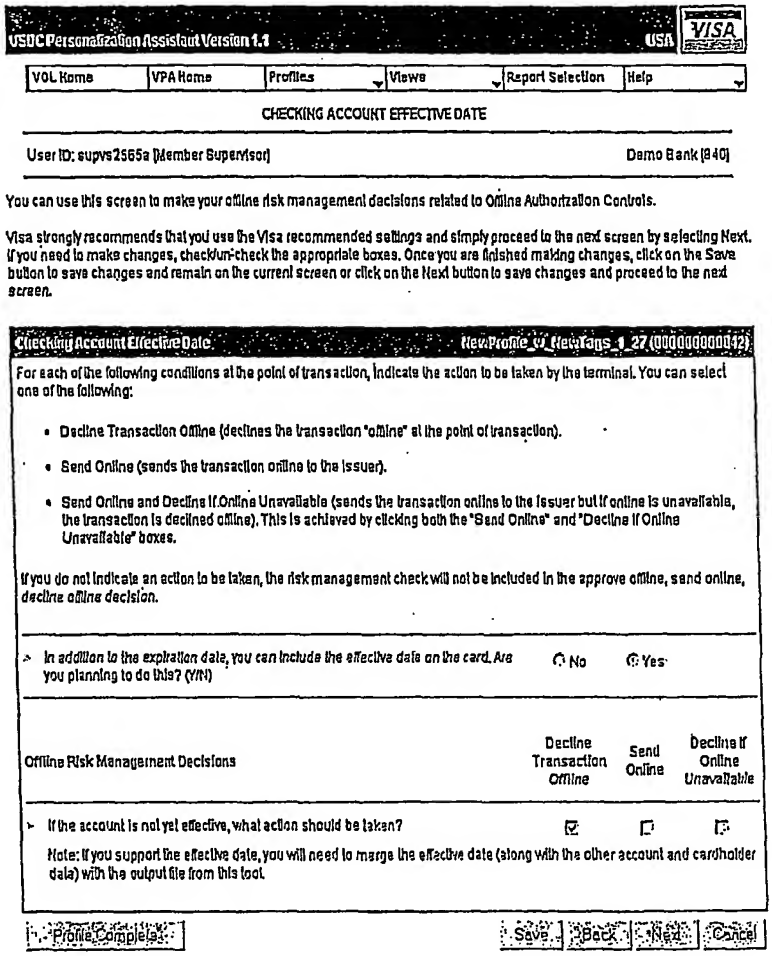


FIG. 26

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.6.10 Offline Risk Management Decisions

This screen allows the user to set either decline offline, send online, or decline if online unavailable for various offline risk management results that may be encountered by the terminal during transaction processing Example include; if the card is new, if card data is missing and if the lower and upper limits specified by the user for offline use have been exceeded.

2704

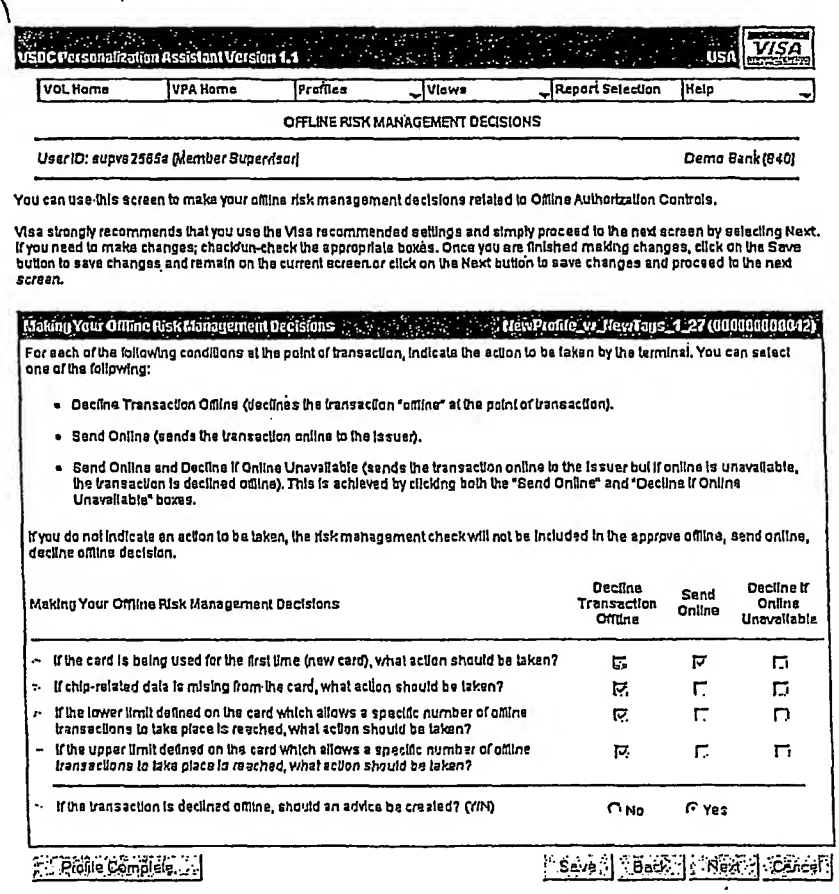


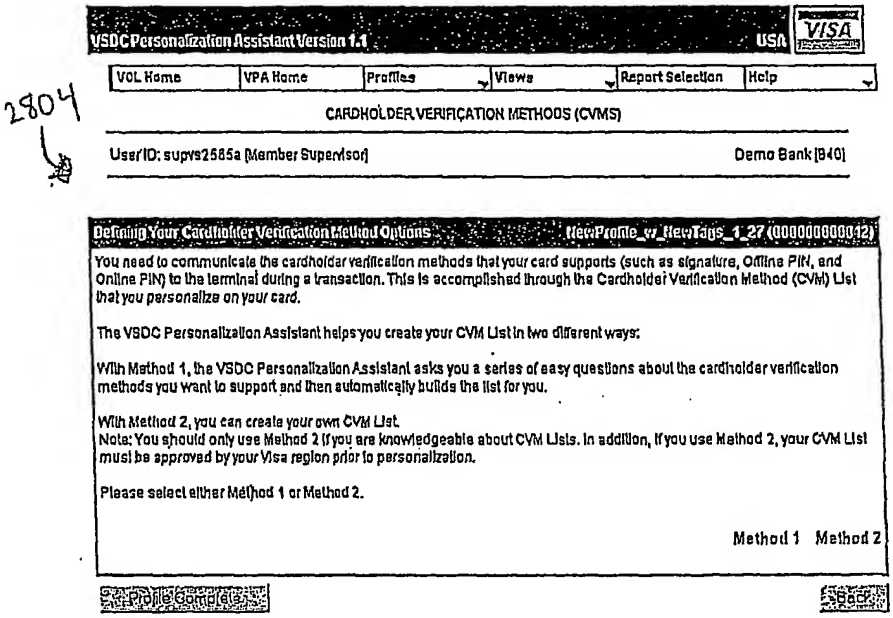
FIG. 27

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.6.11 Cardholder Verification Methods

VPA offers the user a choice of two methods for preparing their Cardholder Verification Methods List.

- Method 1: VPA provides a series of questions, and based on the user's response, the tool will generate the appropriate CVM List.
- Method 2: The user creates their own CVM List.



2804

FIG. 28

Note:

Visa STRONGLY recommends the use of Method 1. Method 2 should only be used if the user is sufficiently knowledgeable about CVM Lists processing. In addition, if Method 2 is used, the Visa regional office must review the chosen CVM List prior to profile activation.

If either of the CVM Methods indicates Offline PIN support, the user will be provided with a screen to allow the entry of the PIN Try Limit and the action to be

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

taken in the event the cardholder exceeds the PIN Try Limit during transaction processing.

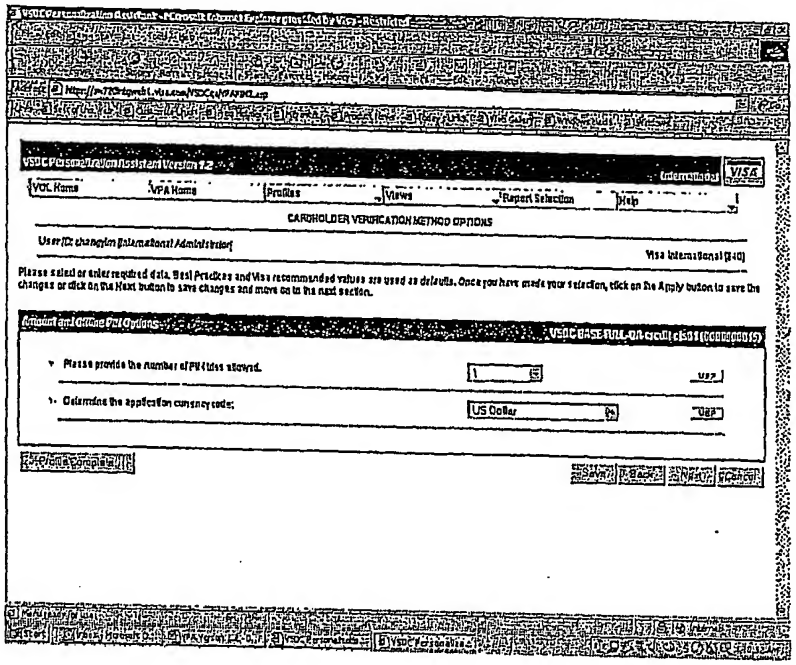


FIG. 29

6.6.11.1 CVM Method 1

CVM Method 1 presents the user with a series of business-oriented questions. The user's responses to these questions will allow VPA to generate the appropriate CVM List. The user can view the CVM List generated by VPA on the Summary screen.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

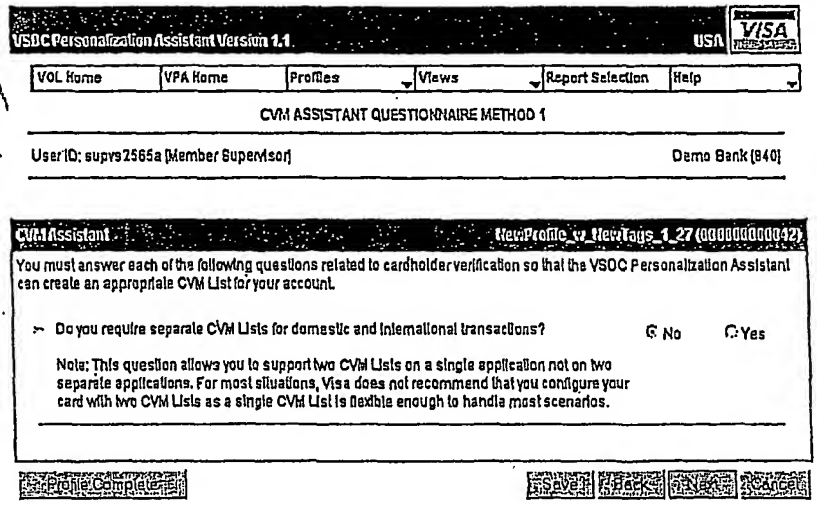


FIG. 30

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

3104

VSDC Personalization Assistant Version 1.1 — USA

VOL Home | VPA Home | Profiles | Views | Report Selection | Help

CVM ASSISTANT QUESTIONNAIRE METHOD 1

User ID: supvs2565a [Member Supervisor] — Demo Bank [840]

CVM Assistant — NewProfile_w_NewTags_1_27 (0000000012)

You must answer each of the following questions related to cardholder verification so that the VSDC Personalization Assistant can create an appropriate CVM List for your account.

* Will you allow your cardholder to be validated using Offline Plaintext PIN?	○ No	◉ Yes
* Will you allow your cardholder to be validated using Offline Enciphered PIN? If you decide to support Offline Enciphered PIN, it is strongly recommended that you also support Offline Plaintext PIN.	○ No	◉ Yes
* At ATMs supporting both Offline PIN and Online PIN, should Offline PIN be used instead of Online PIN?	◉ No	○ Yes
* Will you allow Offline PIN to be used for manual cash OR purchase transactions with cash back?	◉ No	○ Yes
* Will you allow Signature to be used for manual cash and purchase transactions with cash back?	○ No	◉ Yes
* Will you allow Online PIN to be used for purchase transactions without cash back?	○ No	◉ Yes
* Since you answered yes to allow Online PIN for purchase transactions without cashback, do you prefer Online PIN to be used as the cardholder verification method for purchase transactions without cashback when the device supports both Online PIN and signature? Note: When you answer yes, you are stating that you prefer Online PIN to be used for purchase transactions without cash back when the device supports both Online PIN and signature. When you answer no, you are stating that you prefer Signature to be used for purchase transactions without cash back when the device supports both Online PIN and signature.	○ No	◉ Yes

Profile Complete? | SAVE | Back | Next | Cancel

FIG. 31

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

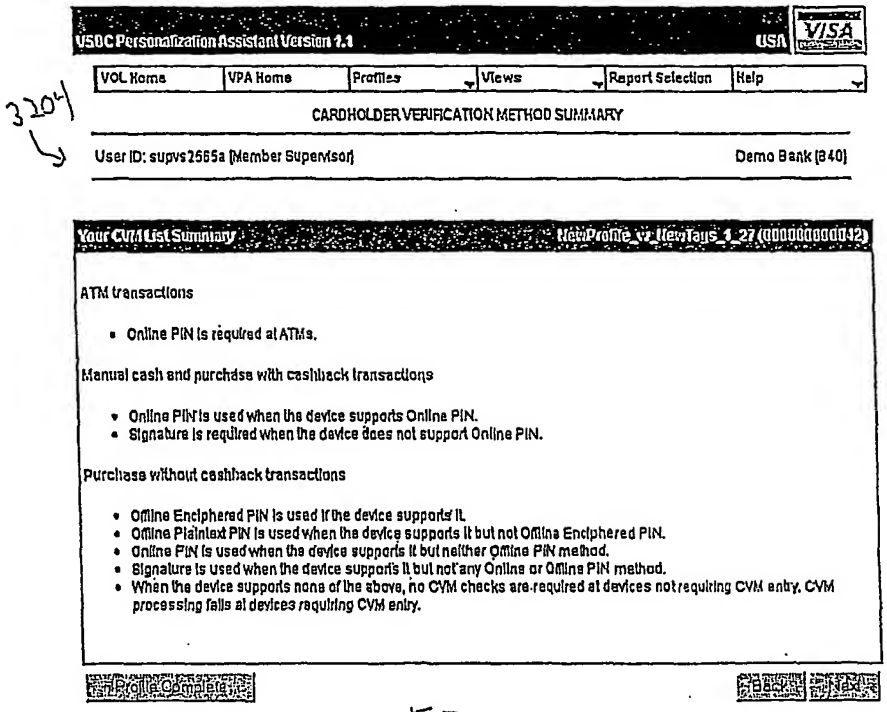


FIG. 32

6.6.11.2 CVM Method 2

CVM Method 2 offers the user flexibility in constructing their CVM List. Because of the complex nature of CVM List processing and the potential for creating problems in interoperability if suitable CVM List is not selected, Method 2 includes a feature to allow Visa to review and validate the CVM List created by the user, prior to its inclusion in the Member profile. The Member profile cannot be activated until the CVM List has been reviewed by Visa.

VPA uses e-mail to facilitate the communication to Visa. The designated Visa contact will be notified by e-mail of a request to review the CVM List. The user will also be notified by e-mail of Visa's approval or decline of the chosen CVM List.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

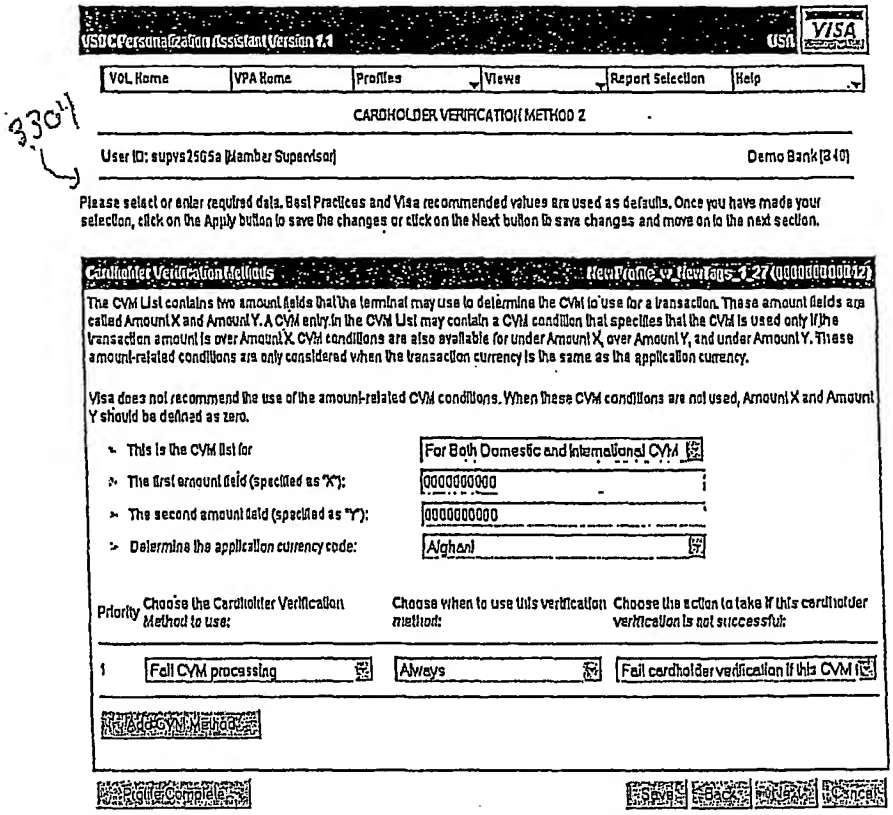


FIG. 33

6.6.12 CVM Risk Management Decisions

This screen provides the options for the user to set either decline offline, send online, or decline if online unavailable for various CVM Risk Management results that a terminal may encounter during transaction processing. In addition, other actions may be requested, such as the blocking of the application, etc. based on results of CVM processing.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

3404

VSDC Personalization Assistant Version 2.1 — USA

VOL Home | VPA Home | Profiles | Views | Report Selection | Help

CARDHOLDER VERIFICATION RISK MANAGEMENT DECISIONS

User ID: supvs2565a [Member Supervisor] Demo Bank: (840)

You can use this screen to make your risk management decisions related to cardholder verification.

Visa strongly recommends that you use the Visa recommended settings and simply proceed to the next screen by selecting Next. If you need to make changes, check/un-check the appropriate boxes. Once you are finished making changes, click on the Save button to save changes and remain on the current screen or click on the Next button to save changes and proceed to the next screen.

Making Your Cardholder Verification Risk Management Decisions — New Profile of Version 1.27 (0000000000042)

For each of the following conditions at the point of transaction, indicate the action to be taken by the terminal. You can select one of the following:

- Decline Transaction Offline (declines the transaction "offline" at the point of transaction).
- Send Online (sends the transaction online to the issuer).
- Send Online and Decline if Online Unavailable (sends the transaction online to the issuer but if online is unavailable, the transaction is declined offline). This is achieved by clicking both the "Send Online" and "Decline if Online Unavailable" boxes.

If you do not indicate an action to be taken, the risk management check will not be included in the approve offline, send online, decline offline decision.

Cardholder Verification Risk Management Decisions	Decline Transaction Offline	Send Online	Decline if Online Unavailable
If cardholder verification is not successful, what action should be taken?	☑	☐	☐
If one of the cardholder verification methods in the card's CVM List is not recognized by the terminal, what action should be taken?	☑	☐	☐
Making Your PIN Pad Risk Management Decisions			
If Offline PIN is required and the PIN pad is not working or not present, what action should be taken?	☑	☐	☐
If Offline PIN is required and the PIN pad is present but the cardholder's PIN is not entered, what action should be taken?	☑	☐	☐
Making Your PIN Try Limit Risk Management Decisions			
If the Offline PIN Try Limit is exceeded, what action should be taken?	☑	☐	☐
If the Offline PIN Try Limit is exceeded on the current transaction and the transaction is declined offline, should an advice be created?	○ No	○ Yes	
If the Offline PIN Try Limit is exceeded on the current transaction, should the application be blocked?	○ No	○ Yes	
If the Offline PIN Try Limit is exceeded on the previous transaction, should the transaction be declined offline?	○ No	○ Yes	
If the Offline PIN Try Limit is exceeded on the previous transaction, should the transaction be transmitted online?	○ No	○ Yes	
If the PIN Try Limit is exceeded on the previous transaction, should the transaction be declined offline if online transmission is not possible?	○ No	○ Yes	
If the Offline PIN Try Limit is exceeded on the present transaction, should the transaction be declined and the application be blocked?	○ No	○ Yes	

Profile Complete | Save | Back | Next | Cancel

FIG. 34

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.6.13 Offline Dynamic Data Authentication

This screen allows the user to determine if additional terminal-based data elements should be used during the Dynamic Data Authentication process. The EMV specifications require that at minimum, a randomly generated Unpredictable Number be used, but the user may specify additional data elements.

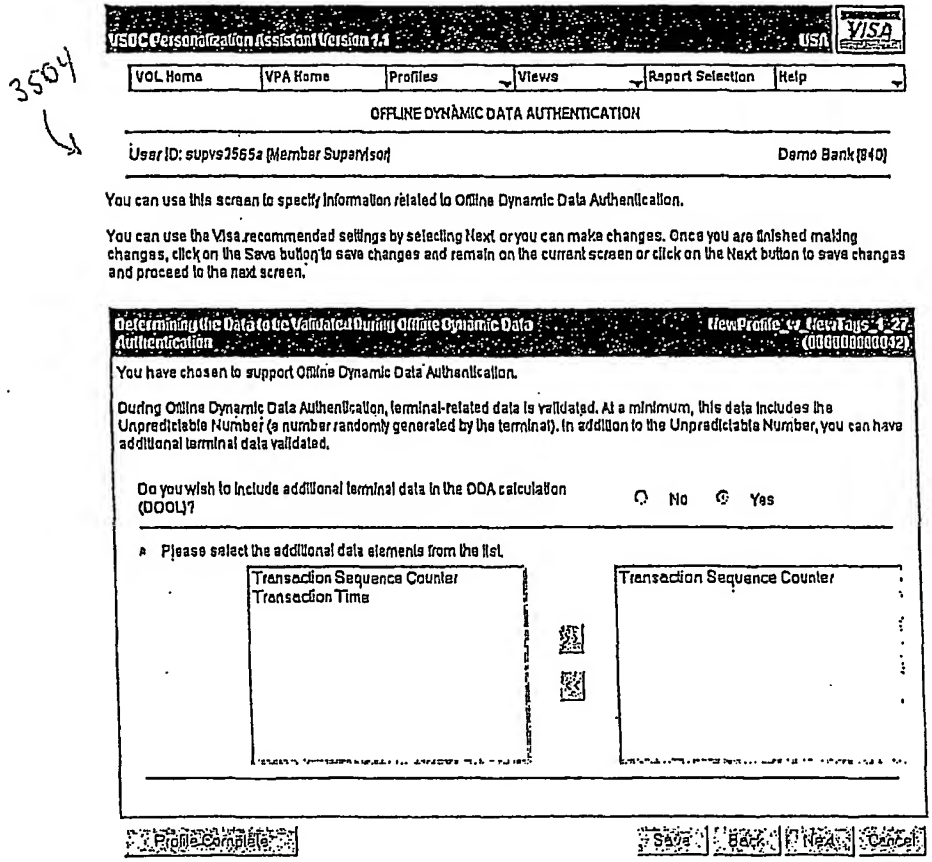


FIG. 35

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.6.14 Offline Data Authentication Risk Management Decisions

This screen provides the options for the user to set either decline offline, send online, or decline if online unavailable for various Offline Data Authentication (SDA or DDA) Risk Management results that may be encountered by the terminal during transaction processing.

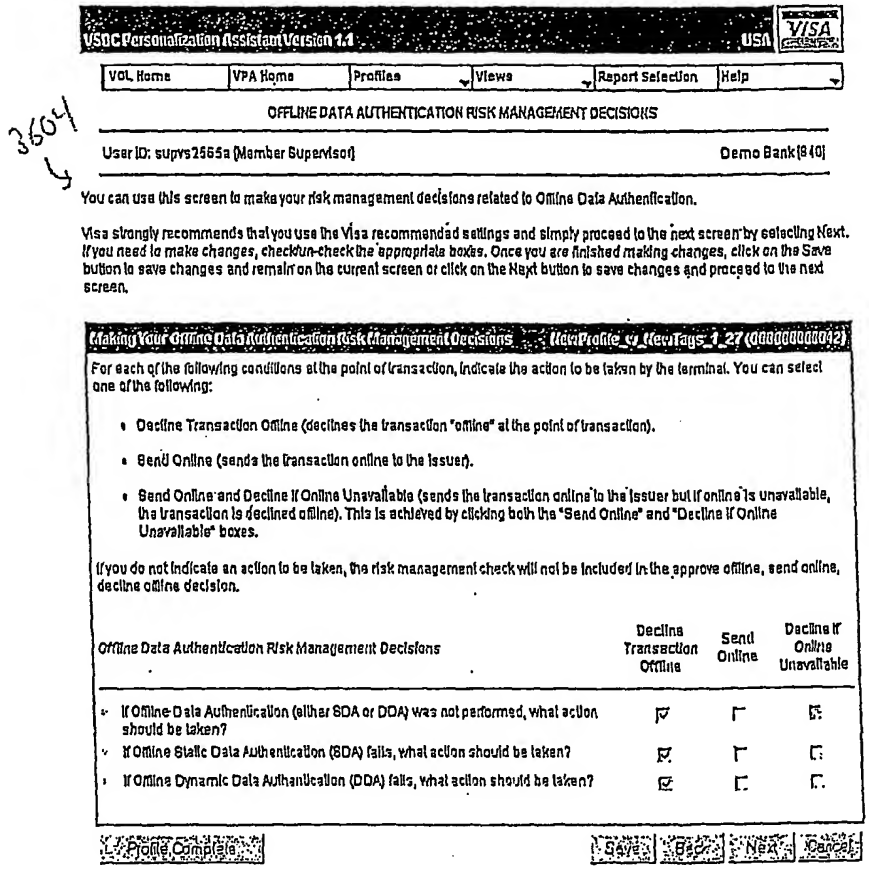


FIG. 36

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.6.15 Card Authentication Options

This screen allows the user to select the appropriate Cryptogram Version Number for the Application Cryptogram that may be sent online to validation by the Issuer or by VisaNet. Visa currently support three version numbers; 10, 12 and 14. The screen provides a detailed description on each of these version numbers.

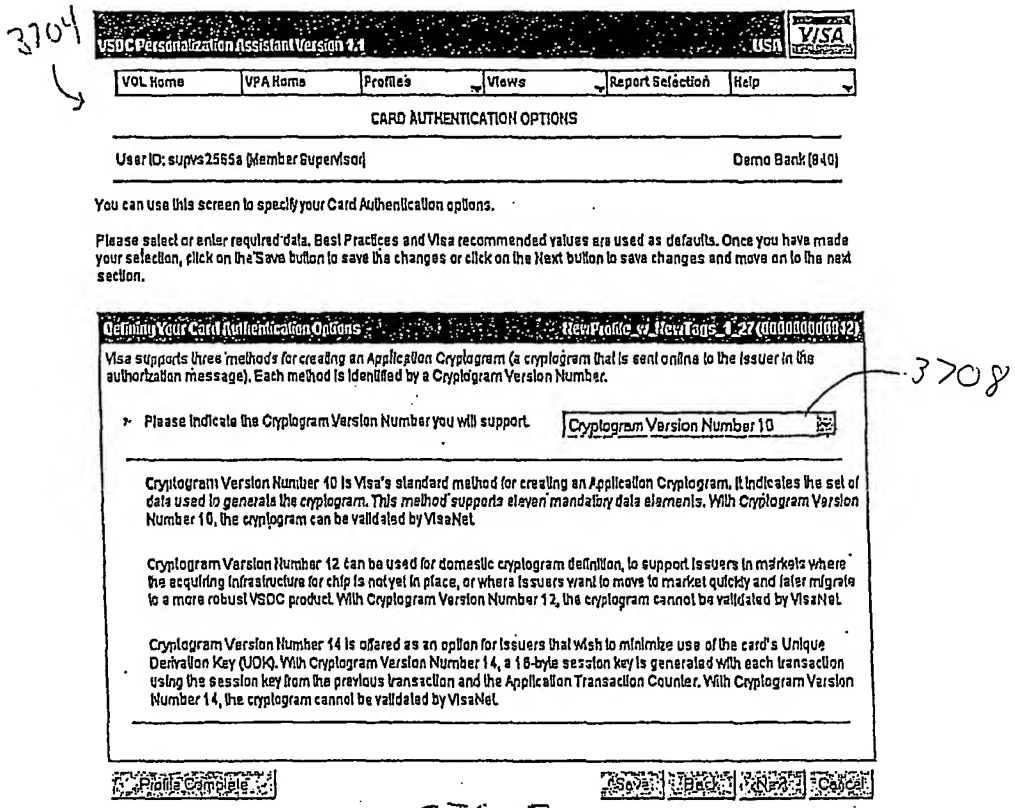


FIG.37

6.6.16 Issuer Authentication Options

This screen allows the user indicate whether Issuer Authentication should be performed as an optional feature or should be mandatory. It also provides the

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

user with additional actions to be performed in the event of a failure of Issuer Authentication.

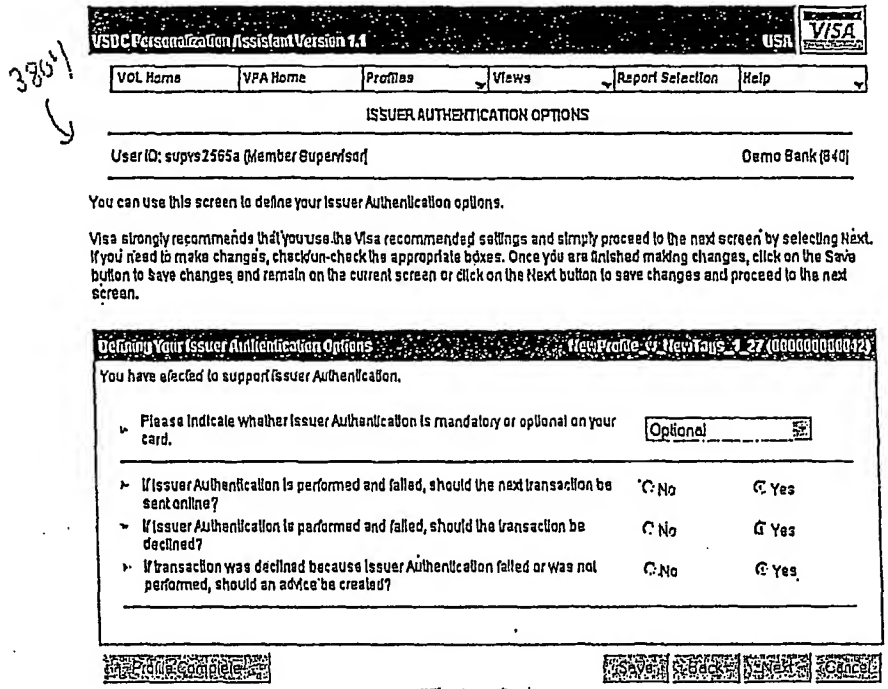


FIG. 38

6.6.17 Issuer Script Risk Management Decisions

This screen allows the user to indicate whether the next transaction should be sent online following the VSDC application's failure to process an Issuer Script.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

3904

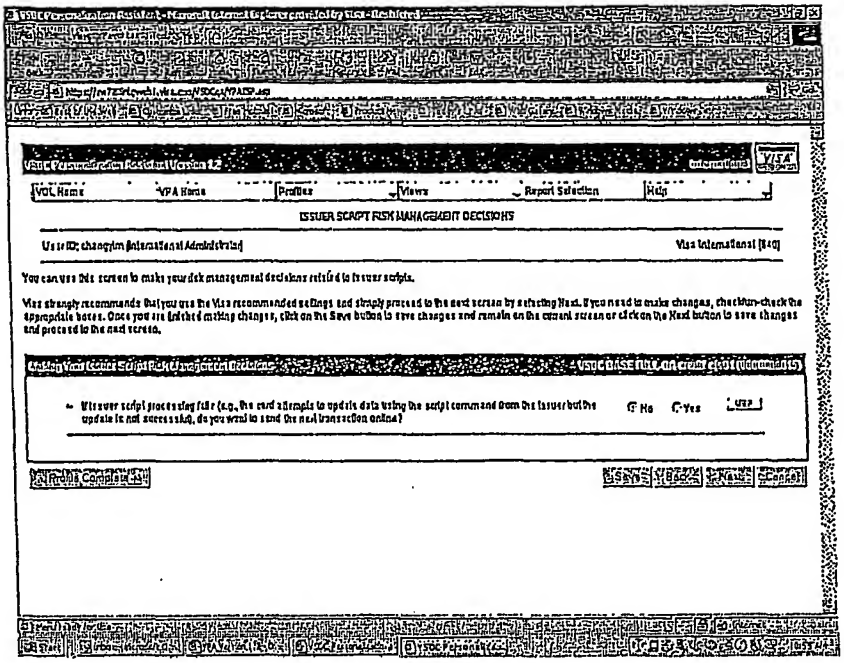


FIG. 39

6.6.18 Visa Low-value Payment Feature

Visa Low-value Payment is an optional VSDC feature that provides quick offline transaction processing for small-ticket purchases in single-currency markets. The VLP Feature Selection screen allows the user to select or change features associated with VLP.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

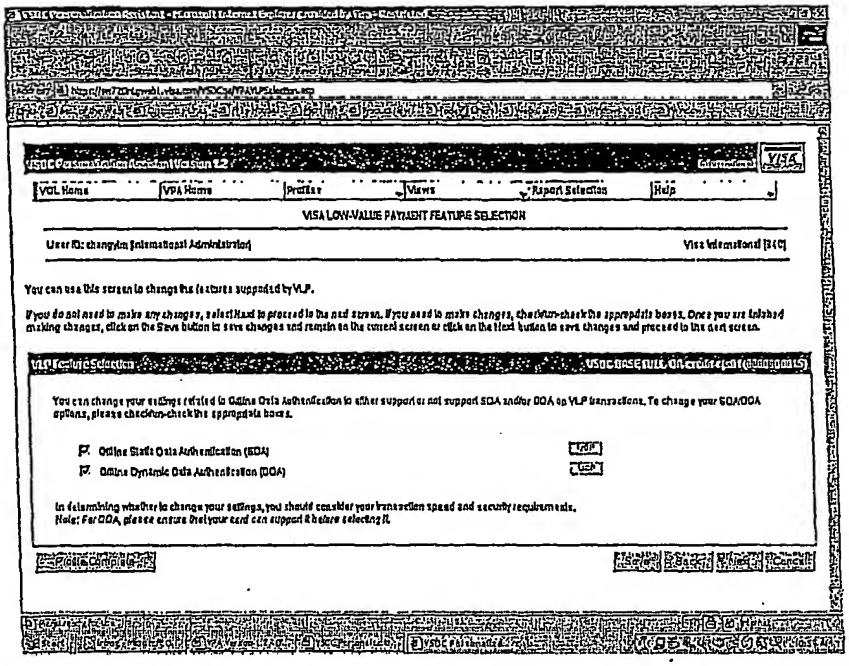


FIG. 40

6.6.18.1 VLP CVM Assistant

This screen allows the user to indicate whether VLP should support the same cardholder verification methods used for VSDC or use separate ones.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

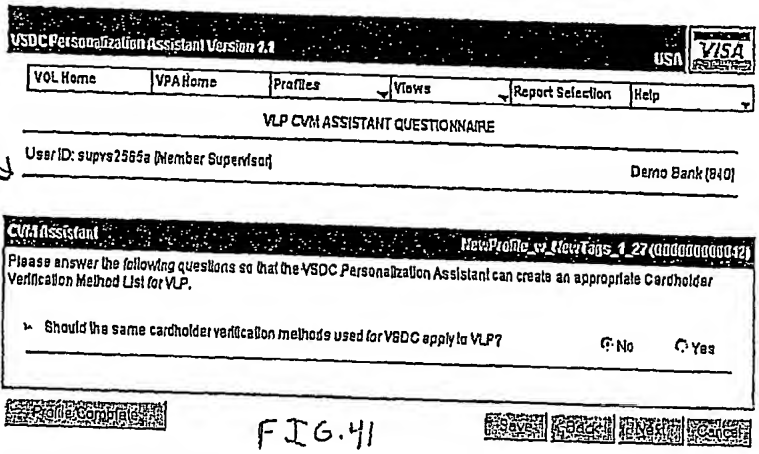


FIG.41

If the user has indicated "no" to having the same cardholder verification methods used for both VSDC and VLP, an additional screen will appear allowing CVM selection.

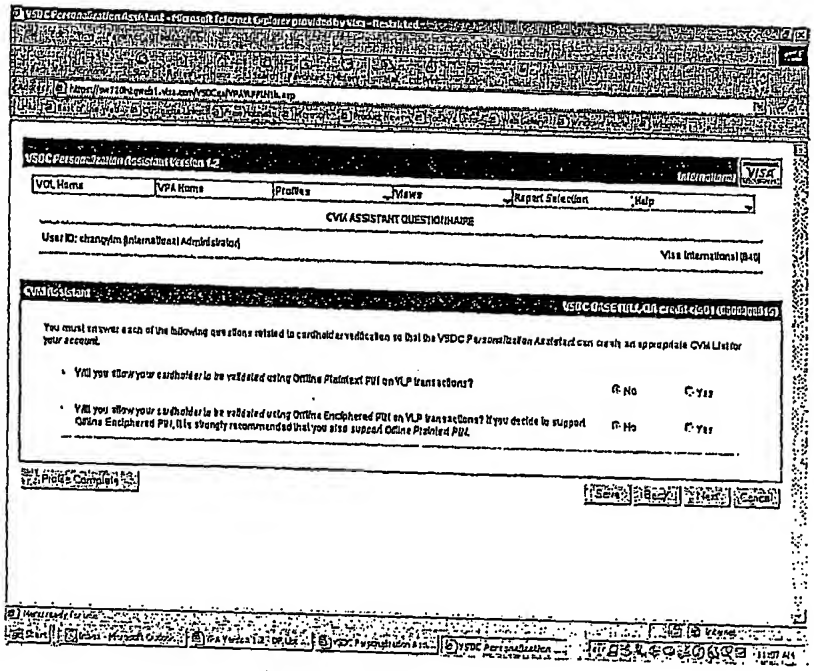


FIG.42

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

Note:

Visa recommends that the same cardholder verification methods used for VSDC be also applied to VLP. Users are therefore recommended to answer "yes" to the question above.

If the user chooses to use the same cardholder verification methods for both VSDC and VLP, the following screen will appear:

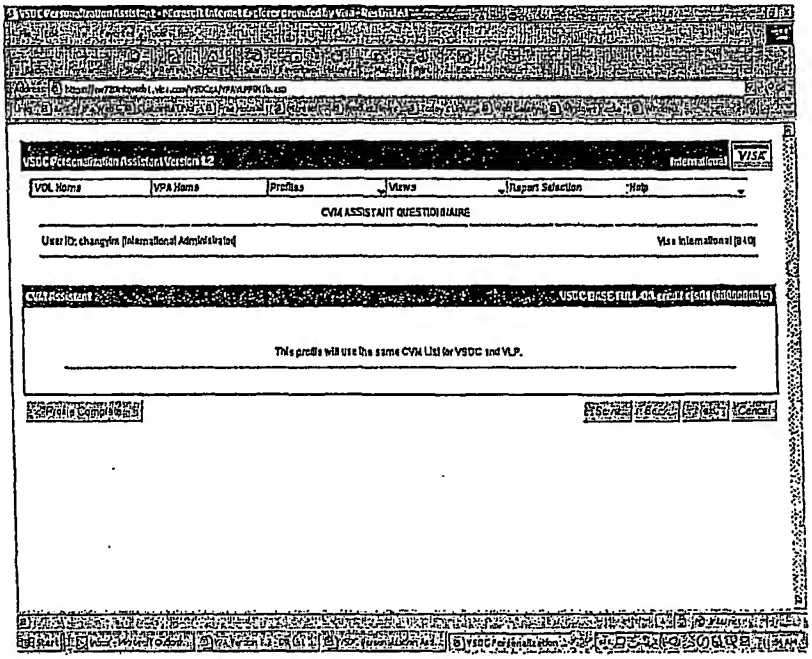


FIG. 43

6.6.18.2 VLP Codes and Limits

This screen allows the user to select the appropriate VLP Authorization Code, VLP Funds Limit and to indicate whether or not VLP Single Transaction Limit should apply.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

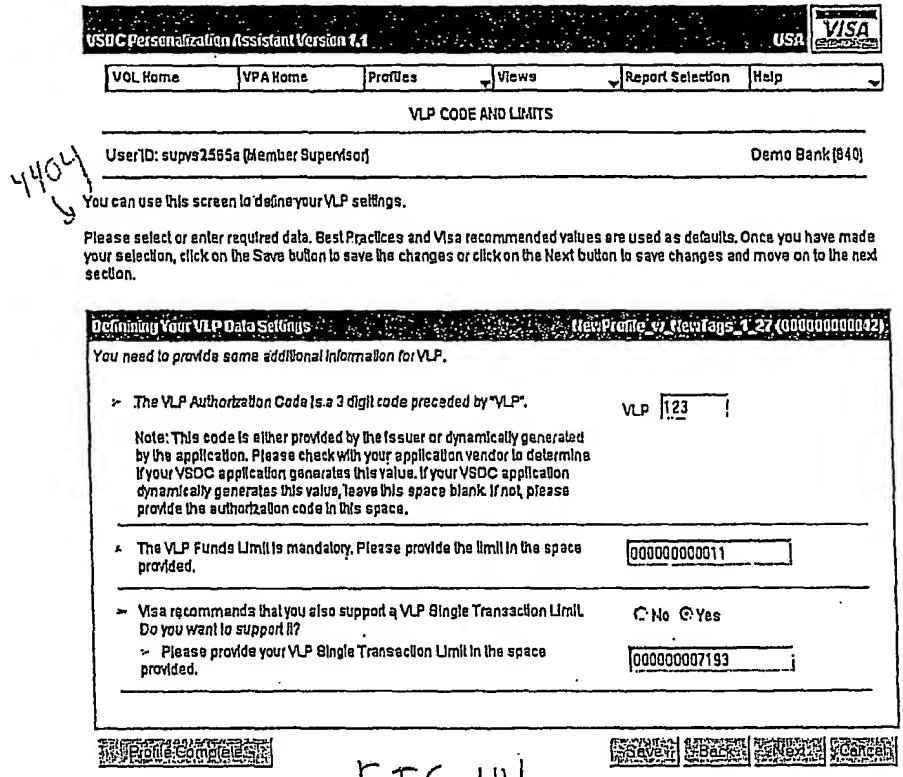


FIG. 44

6.7 VPA Output Options

On completion of the profile creation process, the user will be taken to an Output Options screen. On this screen, the user may choose from a number of options for creating reports or output files.

The reports and output files include:

- Business Report
- Technical Report
- Data Preparation Output File
- VisaNet Stand-In Options Report

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

The contents of all reports are based on the responses made by the user to all the business questions.

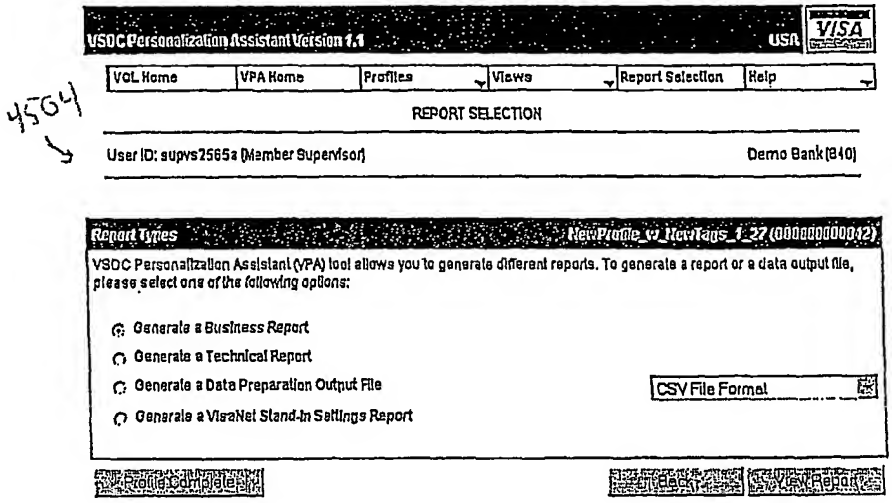


FIG. 45

The user may view, print or save any of these reports. They may also be forwarded to a third-party data preparation service bureau or to the Visa regional office for review.

The process for submitting these reports to Visa for review will be established by the Visa regional office. Users are required to establish their own procedures for submitting Data Preparation Output files to the Data Preparation Service Provider.

6.7.1 Business Report

This report provides a summary of various business decisions and settings. This report also notes any Best Practice violations. Users of this report may include Product Managers, Portfolio Managers, etc.

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

Sample Business Report:

Business Report for FULLVSDC-ISSUER-CREDITPROFILE01

For Account Range:	1111222233334444 to 1111222233334444
Profile Identifier:	000000000017

4604

Magnetic Stripe Image - Usage Control	Best Practice Violation	User Selection
Determine where card can be used and the types of transactions the card should support:		Valid for domestic cash transactions Valid for international cash transactions Valid for domestic goods Valid for international goods Valid for domestic services Valid for international services
Will your cards be valid at ATMs?		No
Will your cards be valid at terminals other than ATMs?		Yes
If you want to specify the preferred name for the account, please select the preferred alphabet for the account.		Latin 1 (Western European)

Magnetic Stripe Image - Product Options	Best Practice Violation	User Selection
Application Identifier for the account		A0000000031010
Preferred alphabet for the account		Latin 1 (Western European)
Enter the preferred name for the account		CREDITO DE VISA
Enter the selection priority for the account		01
Cardholder is required to confirm account selected		No
Enter the preferred language for the account		English

FIG. 46

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

6.7.2 Technical Report

This report provides a summary of various business decisions and settings, supported by technical details such as tag, category, length and values. This report highlights any Best Practice violations. Users of this report may include Member Technical Staff or Visa Regional Support Representatives.

Sample Technical Report:

Technical Report for FULLVSDCISSUERCREDITPROFILE01

For Account Range:	1111222233334444 to 1111222233334444
Profile Identifier:	000000000017
Total Number of Tags:	26

4704

Data Element	Tag	Category	Length	Best Practice Violation	Value
Application Default Action	9F52	VSDC	02		0000 - No Application Default Action has been set.
Application Expiration Date	5F24	VSDC	03		101011
Application Effective Date	5F25	VSDC	03		091011
Application Identifier (AID)	4F	VSDC	07		A0000000031010
Application Interchange Profile (VSDC)	82	VSDC	02		7C00 - Offline Static Data Authentication - Offline Dynamic Data Authentication - Cardholder Verification - Terminal Risk Management - Issuer Authentication

FIG. 47

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

Sample Visa Stand-In Report:

4804

Visa Stand-In Processing Options for FULLVSDC-ISSUER-CREDITPROFILE01

For Account Range:	1111222233334444 to 1111222233334444
Profile Identifier:	000000000017

Processing Options	Report	
This issuer (or processor for issuer) is Full (all chip data)		
Are chip cards issued within any of the account ranges processed under this BIN?	Yes	

Stand-In Conditions	Route-To-Issuer Default*	Stand-In Authorization Response Default*
Transaction exceeds floor limit	No	Approve
Transaction selected randomly for online processing	No	Approve
Cardholder verification failed	Yes	Decline
Unrecognized cardholder verification method	Yes	Decline
Exceeded total, domestic, or international counters	Yes	Approve
Expired Application	Yes	Decline
Application not yet effective	Yes	Decline
Issuer Authentication failed on last transaction	Yes	Approve
SDA failed	Yes	Decline
Offline Data Authentication not performed	Yes	Decline
SDA failed on last transaction and was declined offline	Yes	Approve

FIG. 48

NOTE: This information is CONFIDENTIAL and must be used exclusively for the operation of Visa programs. It may not be duplicated, published, or disclosed without Visa's written permission.

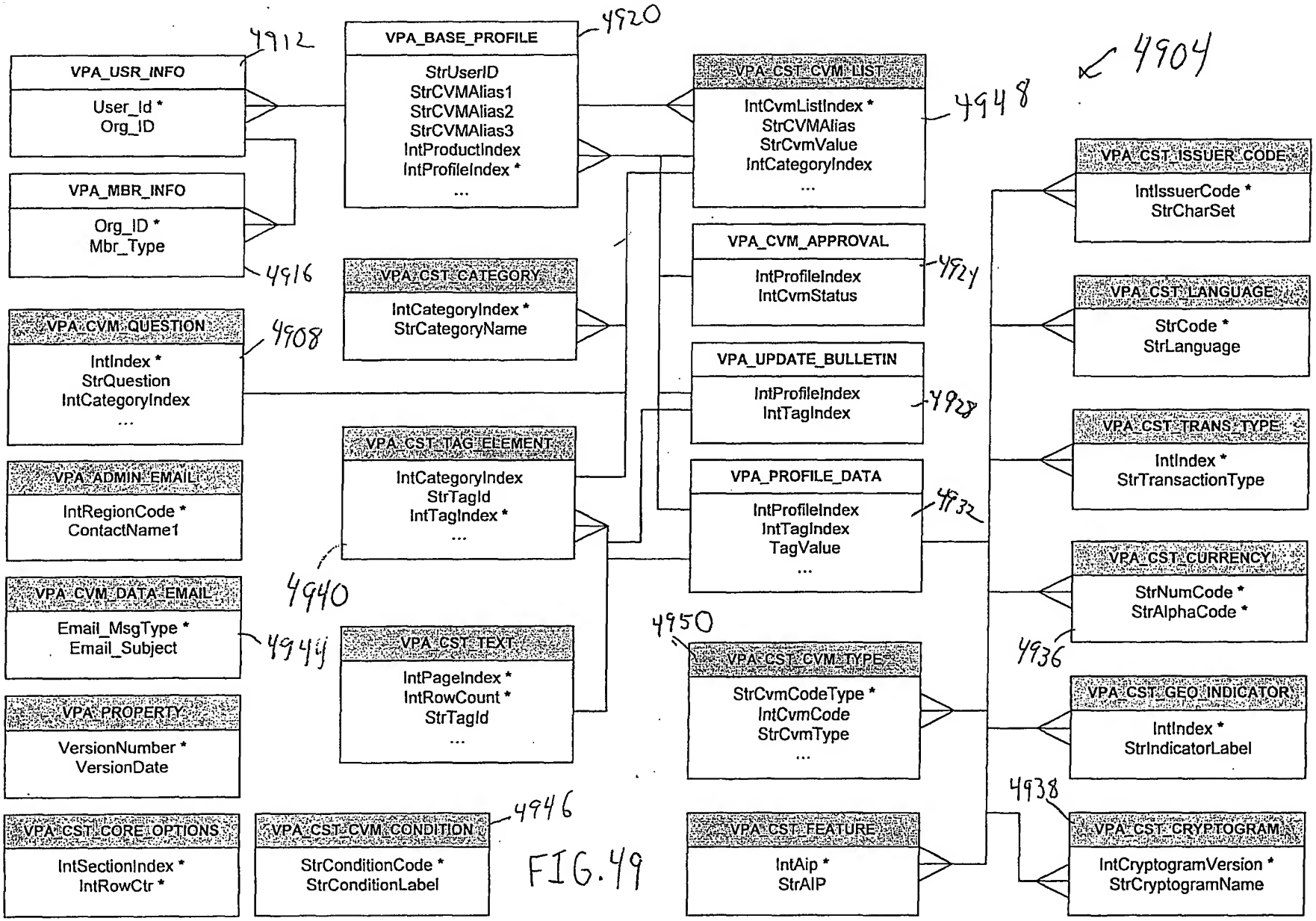

4904
VPA_USR_INFO
User_Id *
Org_ID
4912
VPA_MBR_INFO
Org_ID *
Mbr_Type
4916
VPA_CVM_QUESTION
IntIndex *
StrQuestion
IntCategoryIndex
...
4908
VPA_ADMIN_EMAIL
IntRegionCode *
ContactName1
VPA_CVM_DATA_EMAIL
Email_MsgType *
Email_Subject
4944
VPA_PROPERTY
VersionNumber *
VersionDate
VPA_CST_CORE_OPTIONS
IntSectionIndex *
IntRowCtr *
VPA_BASE_PROFILE
StrUserID
StrCVMAlias1
StrCVMAlias2
StrCVMAlias3
IntProductIndex
IntProfileIndex *
...
4920
VPA_CST_CATEGORY
IntCategoryIndex *
StrCategoryName
VPA_CST_TAG_ELEMENT
IntCategoryIndex
StrTagId
IntTagIndex *
...
4940
VPA_CST_TEXT
IntPageIndex *
IntRowCount *
StrTagId
...
VPA_CST_CVM_CONDITION
StrConditionCode *
StrConditionLabel
4946
VPA_CST_CVM_LIST
IntCvmListIndex *
StrCVMAlias
StrCvmValue
IntCategoryIndex
...
4948
VPA_CVM_APPROVAL
IntProfileIndex
IntCvmStatus
4924
VPA_UPDATE_BULLETIN
IntProfileIndex
IntTagIndex
4928
VPA_PROFILE_DATA
IntProfileIndex
IntTagIndex
TagValue
...
4932
4950
VPA_CST_CVM_TYPE
StrCvmCodeType *
IntCvmCode
StrCvmType
...
VPA_CST_FEATURE
IntAip *
StrAIP
VPA_CST_ISSUER_CODE
IntIssuerCode *
StrCharSet
VPA_CST_LANGUAGE
StrCode *
StrLanguage
VPA_CST_TRANS_TYPE
IntIndex *
StrTransactionType
VPA_CST_CURRENCY
StrNumCode *
StrAlphaCode *
4936
VPA_CST_GEO_INDICATOR
IntIndex *
StrIndicatorLabel
4938
VPA_CST_CRYPTOGRAM
IntCryptogramVersion *
StrCryptogramName

FIG. 49